

Information System Audit and Assurance

Information contained in this work has been obtained by Tata McGraw-Hill, from sources believed to be reliable. However, neither Tata McGraw-Hill nor its authors guarantee the accuracy or completeness of any information published herein, and neither Tata McGraw-Hill nor its authors shall be responsible for any errors, omissions, or damages arising out of use of this information. This work is published with the understanding that Tata McGraw-Hill and its authors are not attempting to render professional services. If such services are required, the assistance of an appropriate professional should be sought.



Tata McGraw-Hill

Copyright © 2005, by Tata McGraw-Hill Publishing Company Limited.

Views expressed in this book are personal and not those of either Reserve Bank of India or of Institute for Development and Research in Banking Technology (IDRBT).

No part of this publication may be reproduced or distributed in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise or stored in a database or retrieval system without the prior written permission of the publishers. The program listings (if any) may be entered, stored and executed in a computer system, but they may not be reproduced for publication.

This edition can be exported from India only by the publishers,
Tata McGraw-Hill Publishing Company Limited.

ISBN 0-07-058569-5

Published by the Tata McGraw-Hill Publishing Company Limited,
7 West Patel Nagar, New Delhi 110 008, typeset in AGaramond at
Le Studio Graphique, 12-C, Sector 14, Gurgaon 122 001 and printed at
Rashtriya Printers

Cover Printer: Rashtriya Printers

RZCQCRLBDXZQL

Information System Audit and Assurance

D.P. Dube

*Faculty
Institute for Development and
Research in Banking Technology (IDRBT)
Hyderabad*

V.P. Gulati

*Professor and Former Director
Institute for Development and
Research in Banking Technology (IDRBT)
Hyderabad*



Tata McGraw-Hill Publishing Company Limited

NEW DELHI

McGraw-Hill Offices

New Delhi New York St Louis San Francisco Auckland Bogotá
Caracas Kuala Lumpur Lisbon London Madrid Mexico City
Milan Montreal San Juan Santiago Singapore Sydney Tokyo Toronto



बारहवीं वित्त आयोग
जवाहर व्यापार भवन,
1, टॉलस्टोय मार्ग, नई दिल्ली-110 001
TWELFTH FINANCE COMMISSION
JAWAHAR VYAPAR BHAWAN,
1, TOLSTOY MARG,
NEW DELHI-110 001

Foreword

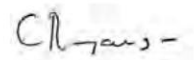
Information Technology has revolutionized the way many organizations function and has brought in a sea change in terms of improved customer service and overall efficiency. Information Systems have facilitated the quick and accurate processing of large volumes of data; they have also been instrumental in bridging large geographical distances.

As the adoption of IT gathers speed, it is imperative that organizations implement a framework for information security that is in tune with their business processes. Organizations are therefore, initiating comprehensive steps towards building appropriate security architecture for their information assets so as to ensure that risks to the organization from Information Systems are mitigated.

One of the tools that effectively address such security concerns is Information Systems Audit (IS Audit). IS Audit in the financial sector assumes special significance. Regulatory authorities the world over have therefore, issued guidelines for mandatory IS Audit. Many universities and research institutions are engaged in identifying various aspects relating to IS Audit and efforts are on to integrate it as a regular inherent process in all organizations which use IT extensively. This book attempts to provide inputs to the personnel engaged in such tasks.

Shri Dube and Prof. Gulati have considerable experience in the introduction of IT in the financial sector. Their initiative to share their knowledge and experience with other practitioners, academicians and researchers through this book is laudable. This book serves as a source of reference for various conceptual issues as also for the operational aspects related to the framing and implementation of a comprehensive IS Audit and Assurance Policy not only in the financial sector but also in its related areas.

I am sure that readers will find this book purposeful and handy.


(C RANGARAJAN)

Preface

"Assurance is two-thirds of Success"

Since time immemorial, people and businesses have depended and thrived on assurances and guarantees. People have looked up to worldly-wise people for advice to ensure that their decisions and actions were right. The same has extended to businesses and organizations— after all, these are but conglomerations of people. Kautilya's *Arthashastra*, composed in 4th Century BC, mentions the extensive use of auditing (a subset of assurance) in the Mauryan Empire. To quote a few lines:

Aksapatala was the head of audit and accounts. He had to conduct the audit of all the government departments, including public enterprises on a regular basis. In the case of misappropriation of money on account of lapses in audit, his office was held solely responsible. Aksapatala had to develop benchmarks of performance, raw material consumption, and performance measurement.

Businesses need third party assurances regarding their assets, business strategies, direction, controls, etc. In the past, such assurances were relatively simple, with most organizations functioning as "stand-alone" units. But, the business environment, as it is today, is completely different. Organizations are gradually becoming IT centric as more and more business processes become IT driven. It is pertinent however, that IT is only a part of what we call Information System (IS), which comprises not only of technology and infrastructure but also of the data associated with them. Perhaps, even more critical is the fact that no organization functions in isolation in today's networked economy. There are completely novel types of assets, processes, resources and information. New things, of course, come with new opportunities, but not without new problems! Now there are new vulnerabilities, controls for which are either inadequate or non-existent.

In such a scenario there is a lot of apprehension among the stakeholders as to whether the Information System (IS) safeguards assets, maintains data integrity, fulfils the organizational goals effectively and consumes resources efficiently. The quest for assurance from a third party is very perceptible.

The idea of writing this book germinated in the year 2001, when we were in the midst of conducting a risk analysis on the Information System of a large

public sector bank in India. This was a part of our assignment for framing Information System security policy for the bank. During this period, we realized that there was a lack of awareness among the stakeholders about appropriate security and assurance processes. This feeling of ours became stronger as we undertook similar assignments for various other banks. Teaching various bankers in related areas viz., Information System Audit, Information Security, IT Governance, Information Risk Management, etc., further accentuated our beliefs. Initially, there was some confusion about the main theme of the book:

Whether it was to be security technology or Information System Assurance and Audit. But it did not take much time for us to zero-in on the current theme. The idea had initially been to dwell on security technology, given the conditions at the turn of the new millennium— Internet was just making its impact felt and Y2K issues had opened up the Pandora's box. However, during the course of the study that went into this book, we realized that security was not a simple tool as in “plug&play”; it had organization-wide repercussions and involved all strata of people and employees.

A network welds together individuals of similar purpose and allows them to pool their efforts to accomplish a common end. However, not all those involved are principled!

As such, security is not a product— it covers an entire gamut of activities, and primary among them are governance, audit and assurance. This realization further strengthened following the incidents of September 11, 2001, and the collapse of Americans' trust in the financial report of private industry (Enron, WorldCom, etc). Even the best of organizations, with the best of security tools, suffered, due to large gaps in security and assurance processes. Their error— treating security in isolation and not following the regular self assessment within.

This realization caused governments and regulatory authorities to take several measures. Notable among them was the passage of the IT Act 2000, by the Government of India, and the Sarbanes-Oxley Act, 2002 (SOX), by the Federal Government of USA. The Sarbanes-Oxley Act has fundamentally changed the business and regulatory environment. The Act aims to enhance corporate governance through measures that will strengthen internal checks and balances, and ultimately, strengthen corporate accountability. Section 404 requires senior management and business process owners not only to establish and maintain an adequate internal control structure, but also to assess its effectiveness on an annual basis. This distinction is significant.

Banking regulators all over the world have also realized the need for Information System Assurance, and issued guidelines for mandatory Information System Audit by qualified personnel. And the banks have risen

to the occasion. The entire market consisting of organizations (the auditee), the auditors, and the regulators are all looking forward to more knowledge in this area... organizations like ISACA (Information System Audit and Control Association), AICPA (American Institute of Certified Public Accountants), and ICAI (Institute of Chartered Accountants of India) are also creating an awareness about the importance of this domain. Several universities in India and abroad have started a regular degree course on Information System Audit. Some, like the University of Hyderabad, have introduced “Information System Audit” as one of the electives in their regular M. Tech. course. The Institute for Development and Research in Banking Technology (IDRBT), an institute established by Reserve Bank of India, has also started a one-year course in Post Graduate Program in Banking Technology (PGPBTM), which possesses a full module on Information System Audit. The number of candidates appearing for CISA (Certified Information System Audit), a globally recognized certification sponsored by ISACA, USA, have increased by almost 10 times in the last three years. Despite such a situation, the number of reference and text books in this area are almost negligible. Hence, we looked over our objectives and felt the need for a publication that would address the issues related to IS audit and assurance instead of pure technology. This is the primary reason for the three years that went into making this book. We feel that the delay has been worth it, as we have culled material from all the major incidents that occurred post-2001. We hope this book provides the relevant insight.

This book is designed keeping in mind the entire Information System Security and Audit industry. It is required by auditors, for their audit purposes, as it gives checklists and practical guidelines on Audit. It is required by Auditees in choosing the right auditor and following appropriate standards. It is required by students of various universities as a reference book on the subject. This is also required by candidates appearing for the CISA examination as this book is per the global standards and permission has already been taken from ISACA, USA for referring to their standard.

There are broadly two methodologies of learning assurance— the top-down and the bottom-up. The former involves understanding the IT control technology philosophy and then developing the assessment methodology, while the latter, the bottom-up approach, first provides the checklist or the assessment methodology and then the control philosophy and technology. Throughout this book, we have followed the top-down approach, with the premise that once the control philosophy is clear, the methodologies required to assess these controls can be safely appreciated.

ABOUT THE BOOK

The book has ten chapters and three appendices.

Chapter 1 provides an overview on Information System Audit and Assurance and, an introduction to the subjects; followed by Chapter 2 on “Internal Control and Information System Audit”, where we discuss the basics of control, and particularly internal controls in the organization. This chapter also covers the various standards of control by different international bodies, with comparisons among them. After these two introductions we come to Chapter 3 on “Conducting Information System Audit”. In this chapter, we give a generic view of the subject and talk about the basic requirement in an IS Audit scenario for both auditee and auditor, with samples and examples from the banking sector.

With these three chapters, we feel, the basics of IS Audit will be clear for the readers. Chapter 4 on “Management Control Review”, deals with what management control is in the Information System environment. What are the roles and responsibilities of the management? What are management control practices followed in the industry and how an IS Auditor audits management control. In this chapter, we give extensive examples from the banking sector and provide a standardized checklist for the auditors.

From management control, we switch over to “Application Control Review” (Chapter 5), where we cover the different types of computer applications, the control requirements, and the guidelines for auditors assessing controls in an application system. Chapter 6 is titled, “Network Security and Control”. In this chapter we dwell on the various types of network technologies and the risks and controls associated with them. A separate chapter, Chapter 7, on “Internet Banking Security and Control” is included because of the relevance of the subject and the relevance of the risks and controls in web-based technology on which lies the basis of internet banking application. A brief introduction on public key infrastructure is included in this chapter.

We then move on to “Operating System Risks and Control”, where we discuss various concepts and access controls in operating system, the file system architecture in the operating system, with checklist for Windows, Linux, and a generic checklist for operating system audit. The next chapter is on “Operation Control Review” where we talk of various risks and controls arising out of operating the Information System. A brief introduction on operational risk from the perspective of the banking and financial sector is also discussed in this chapter. The last chapter is on “Business Continuity and Disaster Recovery Planning Control,” where we discuss the needs for business continuity, business impact analysis, and methodology to assess business continuity preparedness by an auditor.

These ten chapters, are supplemented by three appendices– the RBI checklist for Audit, ISACA standards, and a generic checklists for Information System Audit.

Each chapter has a checklist for conducting audit and four levels of questions (i.e., Review questions, Multiple-choice questions, Discussion and Research questions, and Exercises and Case Studies).

INVITATION FOR FEEDBACK AND COMMENTS

This book has been drawn up with a lot of care and effort to provide readers with an accurate and detailed text. In our endeavor to improve continuously, we would highly appreciate any suggestions, feedback, or comments that would help us in this quest. The same may be directed to the following:

D.P. DUBE
dpdube@idrbit.ac.in

V.P. GULATI
vpgulati@idrbit.ac.in

Acknowledgements

We take this opportunity to thank all those who have helped conceptualize and create this book, particularly the Banking community, colleagues and fellow IS auditors with whom we interacted. Without their views and co-operation, this book would have been incomplete. We would also like to convey our thanks to professionals in the related areas, especially, Mr Sarat Chandra, CISA, CEO, Quad-One Technologies Limited, Hyderabad; Mr S.R. Vijaya Kumar, CISA, General Manager IT, Syndicate Bank, Bangalore; Mr Atul Kumar, CISA, Chief Manager, Syndicate Bank, Bangalore; and Mr P.K. Panda, General Manager, Reserve Bank of India, Mumbai.

Mr Niraj Kapasi, CISA, Ex-President, ISACA, Hyderabad Chapter; Mr Sunil Bakshi, CISA, Chair, Membership Board, ISACA International; Mr A. Rafeeq, CISA, Ex-President ISACA, Bangalore Chapter

S. Ramanarayanan, Shilpa Srivastava— our colleagues and M. John Kinsley— our ex-colleague at IDRBT, helped give shape to the concepts and content. A. Deepti, secretary, IDRBT, was instrumental in typing and formatting the manuscript. Our thanks to them.

Our faculty colleagues from IDRBT, as also colleagues from Reserve Bank of India, have encouraged us in attempting this venture. We are very thankful to them.

Thanks are also in order to our publisher, Tata McGraw Hill, especially Mr Chandra Sekhar, for giving us the opportunity to present our ideas and experience to a wide audience.

We are indeed obliged to Dr C. Rangarajan, Chairman, Twelfth Finance Commission, and Ex-governor, Reserve Bank of India, for sparing his precious time to read the manuscript and write the Foreword. Our profound thanks to him for his views and suggestions.

AUTHORS

xiv *Acknowledgements*

I would like to thank my parents, my parents-in-law, my wife Rashmi, and our daughters Upasana and Aradhana for their unequivocal support and constant encouragement despite the late hours which I had to keep in order to bring out this book on time.

D.P. DUBE

I take this opportunity to convey thanks to my wife Neeta for allowing me to bring home the work relating to this book. My children, Vikram and Aditi, were supportive despite my work encroaching on our time together— thanks to them. And thanks are due to my uncle Dr H.C. Gulati and aunt Mrs Krishna Gulati whose support and encouragement have made me what I am today.

V.P. GULATI

Contents

<i>Foreword</i>	v
<i>Preface</i>	vii
<i>Acknowledgements</i>	xiii
1. Information System Audit and Assurance—An Overview	1
Introduction	1
Assurance Services	2
Need for Assurance	2
Characteristics of Assurance Services	4
Types of Assurance Services	6
Evolution of Information System Audit	6
The Information System— Lifecycle in the Organization	7
The Knowledge Requirement of an IS Auditor	8
The Source of Such Skill	11
Certified Information System Auditor (CISA)	12
Benefits of IS Audit for an Organization	12
Changing Role of Information System Auditors and the Relevance of COBIT	14
Effect of Technology on an Auditor	14
Introduction to COBIT	14
IT Governance and Auditors	15
Summary	18
Review Questions	19
Multiple Choice Questions	19
Discussion and Research Questions	21
Exercises	22
Case Study: To Audit or Not to Audit	22

2. Internal Control and Information System Audit 28

Control	28
Control Framework as Described in COBIT	30
Internal Control	34
Preventive Control	35
Detective Control	36
Corrective Control	37
Compensatory Control	38
Information System Control Procedures	39
Internal Control and Information System Audit	40
Audit Evidence	43
Sampling	44
Computer Assisted Audit Tools and Techniques (CAATTs)	49
Standards of Internal Control	57
Internal Control Framework for Banking Sector	58
Summary	61
Review Questions	61
Multiple Choice Questions	62
Discussions and Research Questions	65
Exercises	65
Case Study: Who Controls Banking?	65

3. Conducting Information System Audit 69

Audit Charter and Engagement Letter	69
A Typical IS Audit Charter	72
Standards, Practices and Guidelines	75
Audit Planning	77
Risk Assessment	81
Information Gathering Techniques	84
Vulnerability	89
System Security Testing	90
Development of Security Requirements Checklist	91
Conducting IS Audit for Banks	100
The Road Map for setting up Information System Audit Framework for the Bank	106

<i>Summary</i>	110
<i>Review Questions</i>	111
<i>Multiple Choice Questions</i>	111
<i>Discussions and Research Questions</i>	113
<i>Exercises</i>	113

4. Management Control Review 114

Management Control	115
Planning	116
Information System Management Architecture	118
Setting up of an Information Technology Framework for a Banking Organization	119
IT Management Framework	121
Role of the Auditor in Evaluating the Planning Process	126
Organizing	127
Procedure	129
Human Resources Policies and Procedures, Relating to the Information System	130
Hiring	130
Promotion of Personnel	135
Personnel Training	135
Cross-training or Staff Backup	135
Employee Job Performance Evaluation	135
Job Change and Termination	136
Outsourcing Practices	136
Organization of Information System Area	146
Leading	149
Controlling	151
Critical Success Factor (CSF)	153
Key Goal Indicator (KGI)	153
Key Performance Indicator (KPI)	154
Auditing Management Control on the Information System	154
<i>Summary</i>	165
<i>Review Questions</i>	166
<i>Multiple Choice Questions</i>	167

xviii Contents

Discussions and Research Questions 168

Exercises 169

5. Application Control Review 171

Application System 171

The Application System 172

Types of Application System 173

Web-based Applications– Thin Clients 175

Thick Clients 177

The Importance of the Application System 179

Application Control 179

Subsystem Factoring of the Application System 179

Keystroke Dynamics 183

Biometric System 184

Terminal Restriction 186

Temporal Restriction 186

Usage Control 186

Audit Trail Control of the Boundary Subsystem 189

Operational Audit Trail of the Boundary Subsystem 190

Existence Control of the Boundary Subsystem 190

Input Subsystem 191

Field Level Input Control 192

Record Level Input Control 194

Batch Level Input Control 194

Data-entry Screen Design 197

Audit Trail Control 200

Processing Controls 201

Other Output Controls 210

Overall Controls 212

Application Control and COBIT 212

Auditing Application Control 213

Substantive Tests 216

Testing the Application System 218

Testing Application Control 219

Concurrent Processing Methodologies 222

Conversion Audit 224

Summary 239

<i>Review Questions</i>	240
<i>Multiple Choice Questions</i>	240
<i>Discussions and Research Questions</i>	242
<i>Exercises</i>	243

6. Network Security and Control **245**

Network— A Tool for Sharing Resources	245
Network Classification	246
Network Topology	249
A Brief Look at the Open System Interconnect (OSI) Model	254
Network Cabling	256
Network Devices	258
The IP Network	260
Threats to the Network	267
Controls to Counter the Threats to Network Security	271
Router Controls	276
Firewall Controls	277
Internal Security	278
IDS	278
Auditing Network	280
A Sample Checklist for Network Audit	288
<i>Summary</i>	301
<i>Review Questions</i>	301
<i>Multiple Choice Questions</i>	302
<i>Discussions and Research Questions</i>	305
<i>Exercises</i>	305

7. Internet Banking—Risks and Controls **307**

Internet Banking— A Multiple-delivery Channel	307
Introduction to Web Technology	308
Hierarchy of ISPs	311
Issues Related to Web Technology	313
Java and Java Beans	313
ActiveX and Active Desktop	314
Client Server vs. Web	314

xx Contents

Delegation of Authority	315
Active Content Problems	316
Authorization	316
Active Content Solutions	316
Types of Internet Banking	317
Features of Internet Banking	318
Generic Architecture	319
Internet Banking in a Distributed Environment	320
Internet Banking in a Centralized Environment	325
Multi-layered Security Model	329
Public Key Infrastructure (PKI)	332
Digital Signature	333
Basics of Penetration Testing	344
Auditing Internet Banking	347
Internet Banking Audit Checklist	348
Outsourcing Issues	352
Web Server Software	358
Web Host	362
Network Environment	365
Summary	369
Review Questions	370
Multiple Choice Questions	371
Discussions and Research Questions	373
Exercises	373

8. Operating System—Risks and Control **374**

Operating System (OS)	374
Types of Operating Systems	375
System Configurations	375
OS Capabilities	377
Functional Components of Operating System	378
Operating System Services	385
User Interface (UI)	390
Access Controls	394
Utility Software	395
Hardening the OS	397
OS Controls	398
OS Security	398

Consolidated Checklist	402
Linux Security Checklist	406
Checklist for Win2k	409
Summary	416
Review Questions	416
Multiple Choice Questions	416
Discussions and Research Questions	418
Exercises	418

9. Operational Control Review **420**

Operation Management– The IS Engine	420
The Functional Areas of Computer	
Operation Management	422
System Administration	426
Network Administration	426
Database Administration	428
Control Requirements for Backup	429
Archiving	430
Off-site Backups	430
Storage of Backups	430
Backup Procedures	431
Backup Techniques	434
Backup Control in the Database Environment	436
Management of IS Operation	438
Controlling the Input/Output (IO) Function	441
Auditing the Input/Output Operation	442
Documentation and Program Library	442
Audit Objective	447
Control over Consumables	448
Maintenance and Control, Related to	
Removable Storage Media	448
Selection of Storage Media	449
Audit Objective	453
Technical Support and Help Desk	454
Elements of SLA	457
Auditing Help Desk and Technical Support	461
Software Maintenance	462
Quality Assurance	465

xxii Contents

Physical and Environmental Security	466
Audit Objectives	471
COBIT and Operational Control	472
Operational Risk from a Banking Perspective	473
What is Operational Risk Management (ORM)	473
Why is Operational Risk Management Important	473
How to Perform Operational Risk Management	474
Provisioning for Operational Risks	475
IS Audit Checklist for Operation Control	476
Summary	484
Review Questions	485
Multiple Choice Questions	486
Discussions and Research Questions	488
Exercises	488

10. Business Continuity and Disaster Recovery (BCP/DR) Planning Control	491

Introduction	491
Need for Business Continuity and Disaster Recovery Planning	492
What is a Disaster in an Information System?	492
BCP vis-à-vis DRP	494
BCP Process	494
Data Backup/Storage	514
Developing an Appropriate Disaster Recovery Strategy: A Case Study of a Banking Organization	520
Business Impact Analysis (BIA)	520
Functionality of CBS, with Internet Banking and ATM, as the Delivery Channels	521
Core Banking Solution	523
Internet Banking	525
ATM Operation	526
Auditing the BCP-DRP	528
Summary	534
Review Questions	536
Multiple Choice Questions	536
Discussions and Research Questions	540
Exercises	541

Appendix A 543

Standardized Checklist for

Conducting Computer Audit	543
1. Business Strategy	543
2. Long-term IT Strategy	543
3. Short-range IT Plans	545
4. IS Security Policy	545
5. Implementation of Security Policy	546
6. IS Audit Guidelines	547
7. Acquisition and Implementation of Packaged Software	548
8. Development of Software: In-house and Outsourced	554
9. Physical Access Controls	557
10. Operating System Controls	560
11. Application Systems Controls	564
12. Database Controls	570
13. Network Management	573
Network Information Security	576
14. Maintenance	579
15. Internet Banking	586

Appendix B 594

- Internet Banking 594
- 3. Review of Internet Banking 596
- 4. Independence 599
- 5. Competence 599
- 6. Planning 600
- 7. Performance of Internet Banking Review 602
- 8. Reporting 608
- 9. Effective Date 608
- Appendix 609
- COBIT Reference 609
- References 610
- 010.010.020 Outsourcing of IS Activities to Other Organizations 611
- 1. Background 611

xxiv Contents

2. Audit Charter	612
3. Planning	612
4. Performance of Audit Work	613
5. Reporting	614
6. Follow Up Activities	615
7. Effective Date	615
020.020.010 Organizational Relationship and Independence	615
1. Background	615
2. Independence	616
3. Planning	616
4. Performance of Audit Work	617
5. Reporting	618
6. Effective Date	618
050.010.040 Effect of Third Parties on an Organizations IT Controls	619
1. Background	619
2. Role of Third-party Service Providers	620
3. Effect on Controls	621
4. Procedures to be Performed by the IS Auditor	621
5. Risks Associated with Third-party Providers	622
6. Contracts with Third-party Providers	623
7. Review of Third-party Provider Controls	625
8. Sub-contractors of Third Parties	628
9. Reporting	628
10. Effective Date	629
060.020.020 Application Systems Review	629
1. Background	629
2. Planning	630
3. Performance of Audit Work	632
4. Reporting	633
5. Effective Date	633

Appendix C

634

A Model Information System Audit Checklist	634
Organization and Administration	634
Program Maintenance and System Development	636

System Development	638
Purchased Software	639
Access to Data Files	639
Access to Data	639
Computer Processing	640
Database	641
Password and Other Online Controls	641
Application Controls	643
Output and Processing	644
Viruses	645
Internet	646
Continuity of Operations	646
References and Suggested Reading	656
Books	656
Reports and Other Publications	657
Websites	657

1

Information System Audit and Assurance—An Overview

-
- ❖ The basics of assurance services
 - ❖ Need for assurance
 - ❖ Characteristics of assurance services
 - ❖ The evolution of Information System audit
 - ❖ The knowledge requirement of an IS auditor
 - ❖ Benefits of IS audit for an organization
 - ❖ Changing role of Information System auditor
 - ❖ Introduction and relevance of COBIT for IS audit
-

INTRODUCTION

You are involved in the decision-making process of a legacy organization, where most of the work-areas are now computerized. The inputs on which you normally depend for taking decisions are not as easily available to you as they were before the advent of the computerized era. You now have to depend on certain computer-savvy employees to provide you the desired information, which they now call DATA. Frankly, you are apprehensive about taking decisions as doubts creep up, like:

- Do I need to know the technology to justify my role?
- How do I know that I am not being misguided by people— who sometimes take me for granted?
- Is power gradually shifting into the hands of those who have access to information? What will happen to my domain knowledge that I have painstakingly acquired?

2 Information System Audit and Assurance

- And finally, am I sitting on the fence because of these apprehensions?

Picture a situation where you want to purchase a commodity from a website, that requires you to pay through your credit card before you receive the goods. A host of apprehensions surface in your mind, like:

- Are the goods authentic? Are they in working order? If I send the money, what recourse will I have if I never receive the goods, or if they are not of the standard or quality as represented?
- Is it safe to disclose my credit card information on the website? Will my name, credit card information, and other particulars be passed on to telemarketing agencies?

While the first reflects your apprehensions about the organization, the second reflects your consciousness as a customer. Although pertinent, there are no concrete answers to these questions. What you really need is assurance!

ASSURANCE SERVICES

The AICPA's (American Institute of Certified Public Accountants) special committee on assurance services defines assurance as:

Independent professional services that improve the quality of information, or its context for decision makers.

The word *Independent* in the definition is crucial as it reflects the unbiased nature of the services in examining and providing information to decision makers.

NEED FOR ASSURANCE

In general, the need for assurance services arises because of:

- Potential bias in providing information; that is the party providing the information may want to convey a better impression than real circumstances merit
- Remoteness between a user and the organization or trading partner
- Complexity of the transactions, information or processing system
- Risk management
- Voluminous data

Bias in Providing Information

Let us take the example of a lending activity, where the borrower provides a financial statement to the lender (financing bank). There is a considerable likelihood that the borrower may submit an inaccurate statement to increase the chances of obtaining the loan. The misstatement could either contain incorrect monetary amounts or inadequate or incomplete disclosure of requisite information. Likewise, the seller of goods and services has a vested interest in convincing you that the product being sold is worth more than a similar product you could obtain from elsewhere. The management of a company can also give misinformation about its financial position to attract investment.

In all the above cases, assurance services will help provide reliable information to decision makers.

Remoteness of Users

Thanks to the Internet, you can now engage in online transactions from the comfort of your home. Although convenient, online buying and selling has certain concomitant disadvantages. For instance, there is an absence of personal interaction with the seller. Moreover, we are unable to physically examine the product before its purchase. This remoteness creates the need for assurance, regarding the trustworthiness of the individual seller, the quality of the product and the authenticity of information received, etc.

Complexity of the System

The complexity and dynamism of the Information Technology (IT) system has undergone a dramatic change during the last decade whereby, IT-enabled applications have become more dynamic. Today, domain knowledge alone may not be sufficient to understand the various ways in which controls are implemented. You probably need to have knowledge of the technology that drives the process. In such a scenario, it is comforting to the management to know that they can seek assurance services whenever needed.

Risk Management

Consider a bank manager's decision to grant a loan to a business concern. This decision will be based on such factors as previous financial relationship with the business house and its financial condition as reflected by its financial

4 Information System Audit and Assurance

statement. If the bank decides to give the loan, it will charge a rate of interest determined primarily by three factors:

1. *Cost of the fund*: This is the approximate rate at which the bank has access to the fund or could be the interest rate on government bonds for the equivalent period.
2. *Business risk for the borrower*: This implies the possibility that the business concern will be unable to repay its loan because of factors such as recession, poor management decisions, or unexpected competition in the industry.
3. *Information risk to the lender*: This refers to the possibility that the information upon which the business decision was based, was inaccurate. An inaccurate financial statement can become a source of information risk.

While assurance has no effect on either the cost of the fund or business risk, it can have a significant effect on the mitigation of Information risk. If the bank manager is satisfied that information risk is minimal after a borrower's financial statement has been certified by an assurator, the overall risk is substantially reduced and the interest rate to the borrower may also be reduced.

Another aspect of assurance, in the case of risk management, is risk transfer whereby part of the risk is transferred to the assurator, like in case of insurance.

Voluminous Data

As organizations grow and the volume of organizational information and data increases, the chances of misstating facts also rise. Sometimes, there may be a need to get an independent third party to identify and give an opinion about such misstatements.

CHARACTERISTICS OF ASSURANCE SERVICES

Assurance services have three critical components:

- An assurance provider
- Information or a process on which the assurance is provided
- A user or group of users/beneficiaries who derive value from the assurance service provided

Information or Process on which Assurance is Given

The items on which assurance is given ranges from the traditional financial statement to the present-day computer system. Assurance can be given on information or a process because to most users, the process is just as important as the information used in a process.

Box 1.1

“And the Oscar goes to....”, “There she is, Miss world...”. Did you know that popular events like the Oscars and beauty pageants are linked with assurance services? Each of these events are observed by well-known assurance experts to assure the viewers that the contests were conducted fairly. So when you become a member of an assurance firm, you might not win an Oscar or a beauty pageant, but you might get very closely associated with these events.

The Beneficiaries

Assurance services can have multiple beneficiaries. Let us take the example of assurance provided by an e-Commerce company. Such assurance directly benefits the company's customer, as the customer is assured of prompt delivery of goods and adherence to quality standards as advertised by the company. Reciprocally, the company also benefit, as the customers will be willing to buy its products. Shareholders and investors too will be able to make judicious decisions regarding the company's shares and investing in it.

Assurance Provider

Assurance may not necessarily be provided only by specialized assurance providers like, Certified Public Accountants (CPAs), or auditors or management consultants. A number of other entities also provide assurance at various stages. For example, when a bank provides a comfort letter regarding a company, it gives assurance to the investors about the credibility of the company. Regulators also provide a unique kind of assurance to the public, although in many instances we do not realize that the services have been rendered. A banking regulator for instance, gives an assurance that it is safe to place deposits in a particular bank.

TYPES OF ASSURANCE SERVICES

Broadly, assurance services can be classified into attestation and non-attestation services. While attestation services involve the evaluation of an assertion made by one party to a third party, non-attestation services do not involve a third party. Traditional statutory audit for instance, is an attestation service which is required as per the statute and by third parties viz., the Government, and the regulators. On the other hand, internal and control self assessment audits are mainly self-imposed and do not involve any third party.

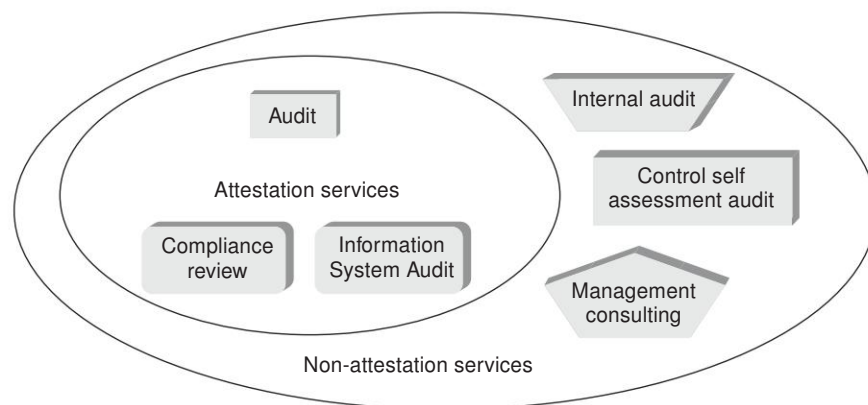


Fig. 1.1 Types of assurance services

EVOLUTION OF INFORMATION SYSTEM AUDIT

Information System (IS) auditing, formerly called Electronic Data Processing (EDP) auditing, evolved as an extension of traditional auditing. The need for IS Audit arose due to several reasons, some of which are:

- Auditors realized that a lack of knowledge of computers had adversely affected their ability to perform attestation functions
- The information processing management recognized that using computer systems was vital to compete effectively with other concerns in the business environment and like other valuable business resources within the organization, had a critical need to possess control and audit ability
- With the growing digitization of information, it was felt that evidence-collection, evaluation, and the entire process of traditional audit needed a paradigm shift

- Professional associations, organizations, government bodies, and regulators recognized the need for Information Technology control and audit

Initially, auditors possessing Information System (IS) skills were viewed as technological experts by the audit staff members, who often sought their help in technical matters. However, gradually, these IS skills became a part and parcel of the audit process and it became vital for auditors to possess these skills.

THE INFORMATION SYSTEM— LIFECYCLE IN THE ORGANIZATION

For any legacy organization, the Information System deployment follows three phases.

- Pervasion*
This is the initial phase where the objective of the organization is the popularization of Information Technology. It is characterized by an unbridled use of IT by the employees.
- Consolidation*
This is the second stage where the organization, after getting a feedback about the widespread use of Information Technology in the organization, tries to consolidate the Information System. This involves ascertaining who uses what, which technology is popular, if there is any constraint in the use of resources, etc.

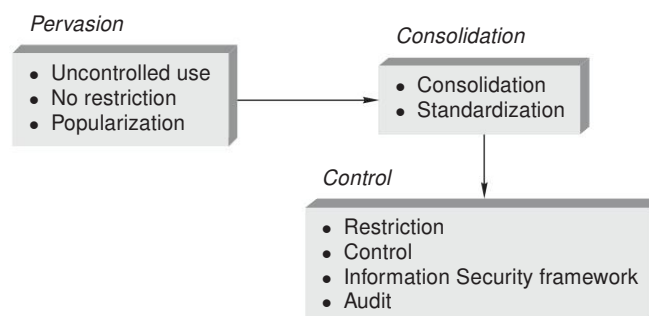


Fig. 1.2 The lifecycle of IT absorption in an organization

- Control*
This is the phase where the organization after consolidating the Information System and ascertaining its uses, tries to put in place

an appropriate mechanism of control and security. In this phase, the organization tries to design an Information System framework that includes the necessary assurance mechanism.

THE KNOWLEDGE REQUIREMENT OF AN IS AUDITOR

Ron Weber in the preface to his book *Information System Audit* wrote that an auditor should be better at business than the client. Similarly, an IS auditor should be more conversant with the Information System than the IS manager in the organization. In a rapidly changing world of IT, to achieve such a high degree of skill although desirable, is an arduous task. To understand the role of an IS auditor, it is important to first understand what IS Audit is.

Ron Weber defines it thus:

Information System auditing is the process of collecting and evaluating evidences to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently.

The above definition tells us that the job of an IS auditor is to give assurance to the company or the auditee that the computer system helps achieve the following objectives:

- Safeguarding assets
- Maintaining data integrity
- Fulfilling the organizational goals effectively
- Consuming resources efficiently

Look at the sequence of the objectives. Data integrity has no meaning in the organization if the assets are not safeguarded. Effectiveness has no meaning unless there is integrity of data and finally efficiency (doing things right) is futile in the absence of efficacy (doing right things).

Let us try and in brief understand the four objectives of IS Audit.

Assets Safeguarding

Information assets are not necessarily what appear on the right-hand side of a balance sheet. In fact, the first and foremost information asset of an organization is the people. Other information assets include data, software, hardware, facilities, and documentation. IT Governance Institute (USA), in its

Governance model, i.e. COBIT (Control Objectives for Information and related Technology) has defined IT resources as being comprised of:

- *Data*: Objects in their widest sense— external and internal, structured and non-structured, graphics, sound, etc.
- *Application Software*: Sum of manual or programmed procedures
- *Technology*: Hardware, Operating System, Database Management System, Network, Multimedia, etc.
- *Facilities*: Resources to house and support Information System
- *People*: Includes staff skills, awareness and productivity in planning, organizing, acquiring, delivering, supporting and monitoring IS and services

Money or capital was not mentioned as an IT resource for classification of control objectives in COBIT because it can be used for investment in any of the other resources. It should also be noted that the *Framework* does not specifically refer to the documentation of all material matters related to a particular IT process. As a matter of good practice, documentation is considered essential for effective control. Therefore, lack of documentation in a particular area, would serve as a cause for further review and analysis for compensating controls in such an area that may be under review.

It would be pertinent to ask if possession of knowledge of IT alone would suffice for an auditor to assure the management that the company's assets are reasonably protected. We will discuss this later in this book.

Data Integrity

Data integrity refers to the accuracy and completeness of data. This is very important from the assurance point of view, as decision makers rely on these data for making strategic decisions. In the event of any inconsistencies or impurities in the data, the management is likely to take inappropriate decisions, thereby putting at stake the interests of its stakeholders.

Effectiveness

Effectiveness simply means doing the right things. From the IS point of view, it implies possession of knowledge of user needs. Auditors must know the needs of the users and the nature of the decision-making environment to assess whether a system reports information in a way that facilitates decision-making by its users.

Efficiency

Efficiency from an auditor's perspective, is doing a job effectively, using minimum resources or using minimal resources to achieve the desired objectives.

Evaluating efficiency however, is a very difficult job as the efficiency of any particular system cannot be considered in isolation.

We can thus safely deduce that the knowledge of IT per se will be insufficient for an auditor to certify the above objectives. He/she must also possess knowledge of traditional auditing which contributes to internal control practices and overall control philosophy. Knowledge of IS management, which helps devise methodologies necessary to achieve successful design and implementation of systems and the field of behavioral science or organizational behavior that provides questions and analysis as to when and why Information Systems are likely to fail due to human errors, are also important requisites for an auditor. Finally, knowledge of computer science enables the auditor to understand the concepts, theory, and formal models that underlie hardware and software designs and serve as a basis for maintaining data integrity or purity.

Box 1.2

The software that does not work

'This software does not work'. 'There are lots of flaws in the software'. These are common complaints of users against their software programmes. Also common are the conflicting views of users about the same software program. Let us take the example of a software application developed in-house and used in various branches of a particular bank. While some branches are fairly happy with the functioning of the software, others complain that the software does not function properly and adds unnecessarily to the overhead expenses of the branch. Gradually the complaints against the software become so intense that the Bank is forced to call for an independent review of the software package by an independent auditor. The auditor first tries to see if there is any disparity between the hardware and system software, used across the branches which could be the reason for malfunctioning of the software in some branches. However, no such incongruity is found. The next task the auditor undertakes is to check for differences in the version of the application software used in different branches. In this case too no disparity is found. Then the auditor decides to take a look at the profiles of the users operating

(Contd)

the software across the branches. The profiles too look almost identical. What knowledge of the auditor then, will enable him/her to find the problem? Ultimately, it turns out that the software has not been functioning properly in certain branches because the person/employee, instrumental in developing this application is disliked by the users of the software in these branches.

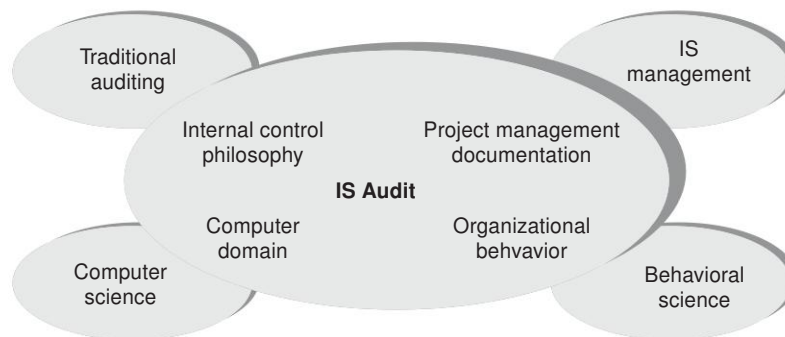


Fig. 1.3 The knowledge requirement for an IS auditor

THE SOURCE OF SUCH SKILL

A majority of the contemporary IS auditors are either traditional auditors with IS skills, or IS specialists with auditing skills. Of late however, study courses focusing on IS Audit in particular, have been introduced by various universities including Indiana and Stanford Universities in USA. Some universities in India are also moving in this direction. For instance, the Institute for Development and Research in Banking Technology (IDRBT), in collaboration with the University of Hyderabad, offers an M. Tech. (Information Technology) course which has an elective on Information System Audit.

The Information Systems Audit and Control Association (ISACA), with over 28,000 members in over 100 countries, is a recognized global leader in IT governance, control, and assurance. Founded in 1969, ISACA sponsors international conferences, training events, and a global knowledge network (K-NET). It also administers the globally recognized Certified Information Systems Auditor™ (CISA) designation, earned by more than 30,000 professionals worldwide and the new Certified Information Security Manager™ (CISM™) designation, and develops globally applicable IS auditing and control standards. The mission of ISACA is to support enterprise objectives

12 Information System Audit and Assurance

through the development, provision and promotion of research, standards, competencies and practices for the effective governance, control and assurance of information, systems and technology.

CERTIFIED INFORMATION SYSTEM AUDITOR (CISA)

CISA, is ISACA's cornerstone certification. Since 1978, the CISA exam has brought forth individuals who excel in the areas of IS auditing, control and security and has since grown to become globally recognized and reputed. There are over 30,000 CISAs worldwide. Information regarding the CISA certification requirements, and exam content are available at www.isaca.org.

BENEFITS OF IS AUDIT FOR AN ORGANIZATION

The importance of control in an organization cannot be ignored at any given point of time. IS auditors are regarded as control advocates in the entire lifecycle of the software and hardware, auditors perform important duties, which benefit the organization in several ways. Some of the benefits organizations receive are:

I. Mapping business control with IT application

An IS auditor can help the organization in ensuring that the necessary business controls are mapped into the application control. Whether the IS auditor should be involved at the project stage of the application or not is a matter of debate, but from the perspective of control it is advisable to involve the internal auditor at the project stage. This way, he/she can help in ensuring that necessary controls are built into the system at the development stage itself. It must however, be ensured that the same auditor is not allowed to conduct a post implementation review/audit of that application.

II. Business process re-engineering (BPR)

The basic difference between automation and computerization is that while in the case of automation, the existing manual process is automated using computers, in the case of computerization, the manual process is re-engineered and then automated using computers. In the latter case, while the absorption of IT is more effectively achieved, there is every likelihood that some basic control may be missed or forgotten in the computerization process, which can have serious ramifications for the organization. For this reason, the IS auditor should be a part of the BPR exercise to ensure that

the basic controls required for the business exist in the re-engineered processes.

III. *The IT security policy*

An IS auditor due to extensive engagement with an organization, is able to say which parts of the policy are being complied with and can also offer suggestions on improving compliance or making suitable changes to the policy. The IS auditor also comes across systems or situations that may not be adequately addressed in the policy and offers guidance on these areas. Proactive IS audit function can make all the difference between an effective IT security policy and one that simply remains a decorative document. From a security and control perspective, an organization without an IT security policy would be considered relatively more secure than an organization with a dormant, non-implementable, IT security policy.

IV. *Security awareness*

An effective IS auditor helps increase levels of security awareness and compliance with security measures among IT users. This also provides motivation to the security officers and system administrators to do their jobs effectively. Consequently, business continuity preparedness also remains at a high level.

V. *Better Return on Investments (ROI)*

IS auditors today, are concerned not just with security and controls, but also with IT governance, which includes performance measurement, value for IT investments, and alignment of IT and business. The profession of IS Audit is gradually being aligned to the profession of IT Governance. Therefore, an IS auditor for an organization helps in effective and efficient use of IT for fulfilling business objectives. Thus, management concerns, like ROI, are taken care of by IS auditor while prescribing IT contracts.

VI. *Risk management*

The domain of IS auditing is gradually moving towards encompassing the domain of risk management and an internal IS auditor is increasingly being seen as a risk management professional particularly in the area of operational risk. Effective risk management is vital for an enterprise's success and therefore, the role of the IS auditor is seen as crucial.

CHANGING ROLE OF INFORMATION SYSTEM AUDITORS AND THE RELEVANCE OF COBIT

Rapid technology changes and development of newer business models based on outsourcing, downsizing, and decentralization have taken businesses and the audit profession through several changes during the last two decades. The changing role of an auditor has been shown in Table 1.1 below:

Table 1.1 Changing role of an IS Auditor

<i>Traditional role</i>	<i>New role</i>
Detection	Prevention
Policeman	Business partner
Focus on audit	Focus on business
Focus on cost	Focus of customer
Focus on function	Focus of process
Auditor	Risk manager
Hierarchical	Team
Quill Pen	Technology

EFFECT OF TECHNOLOGY ON AN AUDITOR

The job of an auditor is to anticipate the directional changes in IT also and the effect these changes and their subsequent implementation may have on business objectives. A key success factor in achieving this objective is for the auditor's role to be fully understood by his business counterparts. Perhaps the most critical area is the identification of weaknesses in the highest strategic planning processes of delicate political issues.

The IT auditor's job is becoming more challenging by the day because the pace of IT deployment is steadily increasing, as companies work to roll out Internet projects in Internet time.

Auditors are also attempting to replace the image of the auditor as the "IT police," with the image of the auditor as someone who has a key role to play in achieving business objectives as a business partner.

INTRODUCTION TO COBIT

One of the major challenges faced by the auditor has been the lack of a common framework within which to operate. This problem was first addressed with

the release of the COBIT (Control Objectives for Information and related Technology) framework, by IT Governance Institute, USA, sponsored by Information System Audit and Control Association (ISACA).

IT GOVERNANCE AND AUDITORS

To meet business objectives, there had to be a common ground for proactive discussion among auditors, IT management, and the board.

COBIT 3rd Edition[®], and the IT governance framework, developed by the IT Governance Institute, addresses these issues through several supporting tools and mechanisms.

These mechanisms have evaluated and defined the role of the auditor within the realm of IT governance.

IT governance activities have thirty-four objectives, one for each of the IT processes. These processes are grouped into four domains, viz.,

- Planning and organization
- Acquisition and implementation
- Delivery and support
- Monitoring

COBIT as a standard for IT security and control practices is not only meant for auditors but also for the management, users, etc. In fact, from a tool of security and control practices, it has evolved into an IT governance tool. COBIT is helpful to managers, users, and auditors in the following manner:

- *Management*: It helps them balance risk and control investments in an often unpredictable IT environment
- *Users*: Helps them obtain assurance on the security and control of IT services provided by internal and third parties
- *IS auditors*: Enables them substantiate their opinions and/or provide advice to the management on matters of internal controls

In the following section, let us discuss specifically the role of auditors in each of the four domains of COBIT.

Planning and Organization

In this area, the board of directors, and management decide the strategy that would help achieve business objectives, and ensure that the technological

infrastructure is in place. This area requires political skill from the auditor, since an IT auditor might have to inform a powerful CIO what has gone wrong under his command and then break the bad news to the senior management. Usually, the board of directors, and the management operate in this domain. The auditor's role here is to evaluate and/or assess whether the functioning of these processes is in accordance with the business objectives.

The only process that the auditor is directly responsible for within this domain is quality management. This process includes the development of a long-term strategic plan, that is in keeping with the mission and vision of the business entity and its stakeholders. The process is also concerned with the measurement criteria to be applied, as well as the identification of specific projects and work plans.

The processes and auditor's duties that are part of this domain are:

- Define a strategic IT plan (evaluate/assess)
- Define the information architecture (evaluate/assess)
- Determine technological direction (evaluate/assess/inform/support)
- Define the IT organization and relationships (evaluate/assess/inform/support)
- Manage the IT investment (evaluate/assess/inform/support)
- Communicate management's aims and directions (evaluate/assess/inform)
- Manage human resources (evaluate/assess/inform)
- Ensure compliance with external requirements (evaluate/assess)
- Assess risks (evaluate/assess)
- Manage projects (evaluate/assess/inform/support)
- Manage quality (evaluate/assess/responsible)

Acquisition and Implementation

To realize the business strategies and tactics, IT solutions need to be identified, developed or acquired. Within this domain, the primary role of the auditor is still to assess the process. However, here he/she should also support the control issues regarding the acquisition and maintenance of application software. The processes and auditor's duties that are part of this domain are:

- Identify automated solutions (evaluate)
- Acquire and maintain application software (evaluate/support)
- Acquire and maintain technology infrastructure (evaluate)
- Develop and maintain procedures (evaluate)

- Install and accredit systems (evaluate)
- Manage changes (evaluate/support)

Delivery and Support

This domain is concerned with the delivery of IT services which include operations through security, training, and support. There is a consensus in the IT governance board regarding the role of the auditor in this process. The role of the auditor here, is to evaluate and assess. However, it is felt that greater involvement of the auditor in the form of providing support in the systems security process would be welcome.

The processes and auditor's duties that are part of this domain are:

- Define and manage service levels (evaluate/assess)
- Manage third-party services (evaluate/assess)
- Manage performance and capacity (evaluate/assess)
- Ensure continuous service (evaluate/assess)
- Ensure systems security (evaluate/assess/support)
- Identify and allocate costs (evaluate/assess)
- Educate and train users (evaluate/assess)
- Assist and advise customers (evaluate/assess)
- Manage the configuration (evaluate/assess)
- Manage problems and incidents (evaluate/assess)
- Manage data (evaluate/assess)
- Manage facilities (evaluate/assess)
- Manage operations (evaluate/assess)

Monitoring

In all the previous domains the auditor is required to check for compliance of processes with quality, and control requirements. This domain requires the auditor to have direct responsibility and provide direct support to the domain's processes. This includes performance measurement for specific indicators defined during the planning process, comparison of these with established parameters and objectives, achievement of critical success factors, and comparison with expected outcomes and stakeholders' expectations.

The processes and auditor's duties that are part of this domain are:

- Monitor the processes (evaluate/assess/support)
- Assess internal control adequacy (evaluate/assess/support)

- Obtain independent assurance (evaluate/ assess/ support)
- Provide for an independent audit (evaluate/ assess/ support)

SUMMARY

With more and more processes of the organizations getting computerized, decision makers are inundated with apprehensions regarding the veracity of the data/information used, on the basis of which they need to take strategic decisions. Customers too feel apprehensive while shopping in the e-Market. Such apprehensions are genuine and reflect the desire of these stakeholders for an assurance from an independent, third-party about the genuineness of the information or goods being used by them. These assurance services when performed by a third-party, for example, traditional audit, are called attestation services. Internal audit of course, cannot strictly be called an attestation service as here the evaluation of the assertion is done by the management and not by a third-party.

Information System Audit is a natural evolution of traditional audit and features the typical characteristics of a phase in the technology absorption of an organization. Looking at the definition of IS Audit by Ron Weber, knowledge requirement of an IS auditor to fulfill the four objectives of asset safeguarding, data integrity, effectiveness, and efficiency, sometimes become a daunting task. Apart from possessing knowledge of computer sciences or IT, the auditor should also have knowledge of project management, organization behavior, and traditional audit. Since IS Audit as a specialized domain of knowledge has gained prominence only recently there are no standard courses offered in this area in most universities. Some universities in the USA like Indiana, and Stanford, University of Queensland in Australia, and some in India (like IDRBT, Hyderabad, in collaboration with University of Hyderabad), offer electives in IS audit. The Information System Audit and Control Association (ISACA), USA established in 1969 is one of the global leaders in IT governance, control, and assurance. The globally accepted certification, Certified Information System Auditor (CISA) offered by them is one of the most well-regarded certifications in the field of IS audit.

Internal IS auditors of organizations are like control advocates. They help the organization in linking the business control to IT application and assure the management that the Information System safeguards assets, maintains data integrity, fulfills the organizational goals effectively, and consumes resources efficiently. It is important to note here that while the role of the auditor is to assure, it is the management that is responsible for ensuring that appropriate controls are placed in the organization. With the rapid growth of

technology, the role of the IS auditor has changed from that of an IT policeman to a business partner. The focus has also shifted from the functional to the process and from audit to risk management.

The release of COBIT (Control Objective of Information and related Technology) by IT Governance Institute (ITGI), sponsored by Information System Audit and Control Association (ISACA), has given a common framework for the auditors to work within. COBIT as an IT governance model/tool is not only used by the auditors, but also by the management and users.

REVIEW QUESTIONS

1. What are assurance services? Why are they needed? What are the three primary reasons for the need for assurance services?
2. What are the characteristics of an assurance provider? Why are these important?
3. What are attestation services? Are these part of assurance services? How are these different from non-attestation services? Explain with the help of examples.
4. Information System Audit is a natural evolution of traditional audit. Explain.
5. Define Information System Audit and explain its four objectives.
6. What are the knowledge requirements for an IS auditor and what are the sources for such knowledge?
7. What are the benefits of IS Auditing for an organization?
8. What is COBIT? How is it important for the stakeholders of the organization?
9. What are the four domains of COBIT? How are these relevant from an audit perspective?
10. Discuss the changing role of an IS auditor in a computerized environment.

MULTIPLE CHOICE QUESTIONS

1. Assurance services involve all of the following except:
 - (a) Improving the quality of information for the purpose of decision making

20 *Information System Audit and Assurance*

- (b) Improving the quality of the decision model used
 - (c) Improving the relevance of information
 - (d) Implementing a system to improve the processing of information
2. Internal auditing is viewed as an integral part of all of the following organizational functions except:
- (a) Risk management
 - (b) Governance
 - (c) Control
 - (d) Operations
3. Which of these functions can be considered an attestation service?
- (a) Management consulting
 - (b) Financial auditing
 - (c) Internal auditing
 - (d) Control self assessment audit
4. To be able to comment on the relative efficiency of the same software across different locations, with the same set of hardware and operated by people of relatively same the level of expertise, the auditor should have the knowledge of:
- (a) Organizational behavior
 - (b) Computer science
 - (c) Project management
 - (d) Traditional audit
5. In case of a Business Process Re-Engineering (BPR) exercise, the role of the auditor is important in assuring that:
- (a) The BPR exercise has got management support
 - (b) There has been appropriate downsizing
 - (c) Controls have been implemented in the IT system
 - (d) The controls in the manual system are appropriately mapped to the IT system
6. Evaluating application control is a part of which domain of COBIT?
- (a) Planning and organization
 - (b) Acquisition and implementation
 - (c) Delivery and support
 - (d) Monitoring
7. "Assess the adequacy of internal control" appears under which domain of COBIT:
- (a) Planning and organization

- (b) Acquisition and implementation
 - (c) Delivery and support
 - (d) Monitoring
8. An IS auditor's role in acquiring and maintaining application software is to:
- (a) Evaluate and support
 - (b) Evaluate
 - (c) Support
 - (d) Assess
9. A member of the Board of Directors of your company, where you work as IS auditor, has told you, in confidence, about the forthcoming changes in the IT Department. What should you do?
- (a) Inform the IT Manager about the impending changes since these are likely to affect his/her department
 - (b) Inform your managers about the forthcoming changes, since your department will need to change the audit plan to accommodate these changes
 - (c) Not inform anybody, since it will amount to a breach of trust
 - (d) Inform both, the IT Manager and your own Manager as the changes are going to affect both departments
10. An IS auditor need not have knowledge of Government or legal restrictions dealing with:
- (a) Computer system practices and control
 - (b) The manner in which computer programs and data are stored and used
 - (c) The organizations and activities of IS services
 - (d) Use of computers in a law enforcement agency
11. In comparison with an external auditor, an internal auditor is more likely to be concerned with:
- (a) Internal administrative controls
 - (b) Cost accounting procedures
 - (c) Operational auditing
 - (d) Internal control

DISCUSSION AND RESEARCH QUESTIONS

1. An external auditor enjoys a higher degree of independence than an internal auditor. Critically examine the statement.

22 *Information System Audit and Assurance*

2. Which economic factors result in an increased demand for assurance services?
3. Efficiency of a computer application does not hold any meaning for the organization unless it is effective. Discuss.
4. 'As an auditor you should be better at business than the clients.' Discuss the statement in the context of the knowledge requirements for an IS auditor.
5. Give examples of the IS auditor's standards of practices? Which organizations have issued standards or guidance to auditors?

EXERCISES

1. Visit the websites of four external audit organizations. Provide a summary of their roles, functions and responsibilities.
2. Visit the website of ISACA and find out the standards for Information System Audit documentation and give your comments.
3. Find out the knowledge requirements for the domain 5 of CISA certification.
4. List ten assurance services and group them into attestation and non-attestation services.

CASE STUDY
TO AUDIT OR NOT TO AUDIT

THE ORGANIZATION

The Progressive Bank is a government-owned legacy bank. It has seen the changing face of the banking sector for over 100 years. Its branches are spread across almost all states of the country. The bank's management has always been willing to accommodate changes. For instance when the government declared that all banks would have to computerize 80% of their business, the bank acted promptly and computerized over a thousand of its branches. In this process, it acquired four different Total Branch Automation (TBA) application software packages, viz. Bankware, Bank123, Banker, and Superbank234. These packages were deployed roughly equally across the fully computerized branches. However, these software packages were not similar. While two of them were using Oracle with Visual Basic frontend one of them, SQL server with Visual Basic, the fourth one was using COBOL with Btrieve

file system. Despite these differences however, all the applications have been running in the Bank for the last three years without any major problems.

THE FUTURE PLAN

In keeping with its name, Progressive Bank has ambitious plans of implementing core banking in a centralized environment. It also wants to explore areas like internet banking, mobile banking, and anything else that would be necessary to retain its market share and sustain its business. As a first step, the bank plans to centralize the operations of 400 branches within a span of two years. To this end, the bank initiated the process of and now is in the final stage of acquiring the software for centralized banking.

AND THEN...

The regulators have issued a guideline that Information System Audit has to be conducted once a year on the applications being used by banks. They have also provided guidelines and sample checklists for such audit. In compliance with these regulatory guidelines, Progressive Bank started the process of empaneling IS auditors for conducting the IS Audit of the four TBA applications running in its branches. As per procedure, the 'Request For Proposal' was floated, stating the eligibility criteria for the bidders/auditors, which were as follows:

- The bidder must be an established company/ firm having national presence
- The bidder company/ firm should have been in the business of auditing in India at least for the last five years
- The annual turnover of the firm/ company should be at least 50 crore rupees
- The bidder company/ firm should have a pool of CISA/ CISSP qualified officials along with persons having domain knowledge in banking
- The bidder company/ firm should not be in the business of selling banking application software including CBS solutions and/ or should not be associated with any entity involved in marketing any such software in India
- The bidder must have conducted similar Information System Audit of Core Banking Software/ Total Branch Automation software in India in at least two other banks

24 *Information System Audit and Assurance*

- The bidder must provide complete details of such audits conducted by it

One of the bidding IS Audit firms, M/s Audit Infotech, satisfied all of the above criteria and also happened to make the lowest (L1) quote. As per the policies and procedures of the Bank, this firm was selected for conducting the IS Audit of the four TBA packages running in the Bank. The auditors, after completing the audit, certified three packages as complying with the regulatory guidelines and checklists. However, in the case of the TBA package Superbank234, they made unfavourable observations which were:

- The software lacks appropriate version control. The version control document submitted, appears to have been prepared by the vendor to satisfy the audit team. It shows that the software changes made were ad hoc and uncontrolled, and did not contain the testing number, and test documents to support them. The vendor of Superbank234, observed the audit team, did not appear to have heard of the famous quotation of Tom Demarco on controlling software changes, “Control change before it controls you”.
- The software does not have date integrity and, as a result, the package permits entries into the system without a day-begin operation being performed.

After raising several other objections, the auditors concluded their report with the following remark:

“In view of the above, we consider the software as not fit for use in the present form by the Bank. The Bank should take immediate care to rectify the problems in the software, otherwise they will be exposed to grave risks, which will prove detrimental to the interest of the depositors”.

Upon receiving the audit report, the bank reported the observations to the vendor and asked him/her to take necessary action, which the vendor eventually did.

THE PROBLEM

Having been informed by the vendor that the rectification in the software as pointed out by M/s Audit Infotech (the auditor) had been carried out, the Bank again asked the auditor to conduct a compliance audit and give a report at the earliest. The audit firm, informed the Bank that its auditors were busy as they were preoccupied with other assignments. Therefore, the audit firm

requested the bank to load the software in its own office so that they could carry out the audit in their office premises itself. The bank then asked the vendor to load the software in the auditor's office, who promptly obliged and the audit exercise started.

At the end of the 11th day (with a break of three days), the auditor again gave a report, which contained not only the irregularities pointed out earlier but also several others. The auditors also pointed out the vulnerabilities of the operating and database management systems on which the software worked. They concluded their report with the following remarks:

“None of the modifications suggested by us in our earlier letter have been made in the software by the vendor. This reflects a very callous and casual attitude. In our assessment, this software is not fit for use in the Bank”.

THE DILEMMA

Progressive Bank was deeply disturbed as this report seriously affected their efforts to implement Superbank234 in other branches. They were also faced with the question of how to continue running the software in the 200 branches where it had been running free of problems so far. A committee was set up to study this matter and present its views.

Before the Committee could commence its meetings, Progressive Bank was faced with some other problems. A letter arrived from the vendor (of Superbank234), alleging unethical practices by the auditor, M/s Audit Infotech. Also enclosed was an audit report on the software (Superbank234) prepared by a third party auditor appointed by the vendor. This audit report was in total contradiction to the report of M/s Audit Infotech appointed by the Bank. It clearly stated that, “All the deficiencies pointed out by M/s Audit Infotech in this application software had been taken care of by the vendor and the software as such had no deficiencies which could be detrimental to the interest of the Bank or to its customers. It can be safely operated as a Total Branch Automation Package in the Bank”.

The audit firm which had been appointed by the vendor possessed all the requisite qualifications and experience to conduct the IS audit, as required by the bank in their RFP for empanelment of auditors. The vendor (of Superbank234), in his letter alleged that:

- The bank had used the TBA software audit as a ploy to influence how orders for the software would be placed. This audit, wrote the vendor, was carried out to probably prevent them from receiving further orders from the Bank.

- The auditor and some bank officials had got together and used the audit report as a tool to oblige other vendors.
- The points raised by the auditors in the final report were frivolous and were made with the intent of giving an unfavourable report.
- The auditor had demanded a bribe from the vendor to make a report in the favour and the vendor had evidence to prove the same.

The Bank was in a fix. The committee discussed the matter at length, and finally decided to call in M/s Audit Infotech to audit the software in front of the bank officials at the bank's headquarters. Accordingly, the auditors were asked to come and start the audit exercise. The auditors however, expressed their inability to do so as they perceived a threat to the lives of their team members from the vendor.

The Bank is now at its wits end. Several questions arise:

- What would be the best course of action in the given circumstances?
- Who is correct, the auditor or the vendor? How should the issue of auditing the software be resolved?
- Should the Bank get involved in sorting out the differences between the auditor and the vendor?
- Can the Bank rely on the audit report of the third party auditor appointed by the vendor?
- If the auditor is in fact involved in unethical practices, can the Bank rely on the reports given by the same auditor for the other three software packages?
- Should the Bank have all its software packages audited all over again?
- What should the Bank do if the vendor is found guilty of making false allegations and the software actually turns out to be risky to operate?
- Ultimately, how should the Bank work towards implementing the Government and Regulatory guidelines of achieving 100% computerization, the deadline for which was closing in?
- If the process adopted as per guidelines given by the regulators failed to ensure the selection of dependable auditors, how else could the Bank select them?
- Should the Bank develop its own internal team of software audit experts?
- Should the Bank develop its own software package and stop outsourcing?

- Should there be a common body that can resolve such issues for all banks?

All these problems confront the management and they are in urgent need of some expert advice.

Disclaimer: All names of characters and companies occurring in this case study are fictitious. Any resemblance to existing entities is purely coincidental and unintentional.

2

Internal Control and Information System Audit

-
- ❖ The basics of control
 - ❖ Control framework of COBIT
 - ❖ Control classifications
 - ❖ Compensatory control
 - ❖ Information System control procedures
 - ❖ Audit risk and materiality
 - ❖ Audit evidences
 - ❖ Computer Assisted Audit Tools and Techniques (CAATTs)
 - ❖ Audit sampling
 - ❖ Various standards of internal control and a comparative analysis
-

CONTROL

“Control” is not a new word. From time immemorial, it has been the endeavor of mankind to somehow or the other control the dynamics of this complex, ever- changing society. Although the basics of control are eternal, their implementation has differed across the manual to the now automated environment. The control theory in the high level systems, which is probably more than a hundred years old, defines control as “*any input given to a dynamic system to produce a desired output*”. Here, the words *dynamic* and *desired output* are very important. From them we can deduce the following:

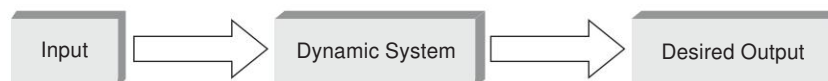


Fig. 2.1 Control as described in the control theory

Dynamism of the System and Control Requirement

In a static system, control is not required and the more its dynamism, the greater will be the control requirement of the system. In the case of a computer system therefore, control is not required if it is not being used for any application or is switched off. However, as its complexity increases, its control requirement will also rise. This implies that lesser control is required for a stand-alone system and greater for one which is connected to the network or Internet, etc.

Knowledge of Dynamism of the System Makes Control Effective

The predictability of the complexity of diseases has helped in the development of vaccines to prevent and cure these. Similarly, in a computer system, control measures would operate effectively if the dynamism and complexity of the system were known. In a very complex computer system for instance, prevention measures like firewall, etc., alone cannot provide the desired level of security as the dynamism of these systems is very high.

The Input should be Directed towards Achieving the Desired Output

This means that if the inputs are not focused and directed towards specific outputs, then the control mechanism not will be successful. Since there are no thumb rules or measures for controlling a complex and dynamic computer system, each input or control measure should be directed towards achieving a specific output.

The Output should be Evaluated for Giving Further Appropriate Input to the System

Box 2.1

Take the example of an automobile driving system, which is comprised of an accelerator, carburettor, and engine. Here, the input (command signal) is the force applied on the accelerator pedal and the automobile speed is the output (controlled) variable. The route, speed, and

(Contd)

acceleration of the automobile are determined and controlled by the driver by observing traffic rules, and road conditions and by manipulating the accelerator, clutch, gear lever, brakes, and steering wheel, etc. Suppose the driver wants to maintain a speed of 60 km per hour (desired output), he/she would have to accelerate the automobile for achieving the desired speed and would then have to maintain it by holding the accelerator steady. There will be no variations in the speed of the automobile, so long as there are no gradients or other disturbances along the road. The actual speed of the automobile is measured by the speedometer and indicated on its dial. The driver reads the speed dial and mentally compares the actual speed with the desired one (*evaluation*). Any discrepancy between the two is rectified by increasing or decreasing the speed.

This example shows how the input can be effectively altered on the basis of evaluation of actual performance to achieve the desired output. The same is true for a complex computer system. When an anti-virus software is deployed, it acts as a detective, or preventive, and sometimes even a corrective control. The output can be observed by regular virus scanning, etc., to see whether the desired output has been achieved or not. When the output is not of the desired level, it means the system is infected with some viruses, which could not be prevented, detected or corrected by the anti-virus software. Based on such evaluation and feedback, patches can be loaded or new anti-virus software or other input deployed. Therefore, feedback and evaluation of the output can enable us to use inputs in a way that would help achieve the desired result.

Although the control described in the control theory is for high level systems and probably more than 100 years old, it holds good for any kind of control whether general or computer control. Now let us discuss 'control' as described in the COBIT and compare it with that described by the control theory.

CONTROL FRAMEWORK AS DESCRIBED IN COBIT

The basic concept of the COBIT framework is that control in IT is approached by looking at information that is needed to support the business objectives or requirements and by viewing information as the result of the combined application of IT-related resources that need to be managed by IT processes.

The basic control framework is depicted in Fig. 2.2.

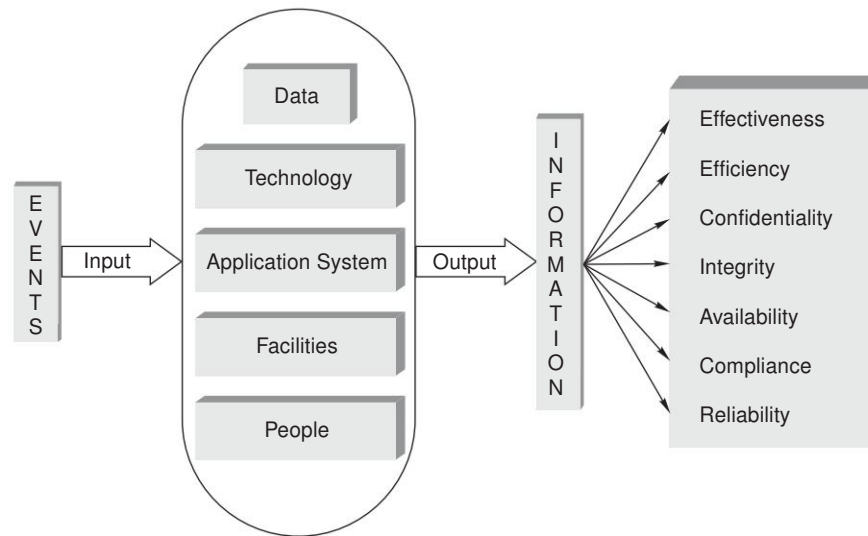


Fig. 2.2 Dynamic Information System

From the above exhibit it may be observed that the input is given to a dynamic Information System, which consists of:

- *Data*, which are objects in their widest sense i.e., external, and internal, structured and unstructured, graphics, sound, etc.
- *Application System*, which is the sum of manual and programmed procedures
- *Technology*, which covers hardware, operating systems, database management systems, networking, multimedia, etc.
- *Facilities*, the resources to house and support Information Systems
- *People*, which includes staff skills, awareness and productivity to plan, organise, acquire, deliver, support, and monitor Information Systems and services

The output produced is again information, which needs to conform to certain criteria, which COBIT refers to as 'business requirements for information'. Such criteria can be placed under three broad categories i.e. *quality*, *fiduciary*, and *security*.

Quality has been retained primarily for its negative aspects (no faults, reliability, etc.), which is also captured to a large extent by the integrity criterion. The positive, but less tangible aspects of quality like style, attractiveness, "look and feel," performing beyond expectations, etc. were, for a time, not being considered from an IT control objectives point of view. The premise is that

the first priority should go to properly managing the risks as opposed to the opportunities. The usability aspect of quality is covered by the effectiveness criterion. The delivery aspect of quality was seen as overlapping the availability aspect of the security requirements and also to some extent effectiveness and efficiency. Finally, cost is also considered as covered by efficiency.

For the *fiduciary* requirements, COBIT did not attempt to reinvent the wheel—COSO's (Committee of Sponsoring Organizations of Treadway Commission's Internal Control Integrated Framework) definitions for effectiveness and efficiency of operations, reliability of information, and compliance with laws and regulations were used. Reliability of information was expanded to include all information, not just financial.

With respect to the security requirements, COBIT identified confidentiality, integrity, and availability as the key elements. It was found that these three elements, are also used worldwide in describing IT security requirements.

Starting the analysis from the broader quality, fiduciary and security requirements, seven distinct, but clearly overlapping categories were formed. COBIT's working definitions of these are—

Effectiveness: is concerned with information being pertinent to the business process as well as being delivered in a timely, correct, consistent, and usable manner.

Efficiency: is concerned with the provision of information through the optimal (most productive and economical) use of resources.

Confidentiality: is concerned with the protection of sensitive information from unauthorized disclosure.

Integrity: relates to the accuracy and completeness of information and to its validity, in accordance with the business values and expectations.

Availability: relates to information being available when required by the business process in the present and in future. It is also concerned with safeguarding necessary resources and associated capabilities.

Reliability: deals with complying with those laws, regulations, and contractual arrangements to which the business process is subject, i.e. externally imposed business conditions.

Compliance: relates to the provision of appropriate information to the management, to enable it to operate the business entity and exercise its financial and compliance reporting responsibilities.

Now, let us compare the COBIT's control framework with the control theory described above. In the case of the former, the input is given to a dynamic Information System, which consists of data, application, technology, facilities, and people. The output produced thereof, is evaluated to ascertain whether it fulfills the business requirement of information, viz. effectiveness, efficiency, confidentiality, integrity, availability, reliability, and compliance. Based on this evaluation, further input is given to the same system for getting the desired output. COBIT provides a sound framework to organizations to satisfy themselves that the information they get is what they need.

The COBIT framework consists of high-level control objectives and an overall structure for their classification. The underlying principle for the classification is that there are, in essence, three levels of IT efforts when considering the management of IT resources. Starting at the bottom, there are the activities and tasks needed to achieve a measurable result. While activities have a lifecycle concept, tasks are more discrete. The lifecycle concept has typical control requirements that are different from those of discrete activities. Processes are then defined one layer up as a series of joined activities or tasks with natural (control) break. At the highest level, processes are naturally grouped together into domains. Their natural grouping is often confirmed as responsibility domains in an organizational structure and is in line with the management cycle or lifecycle, applicable to IT processes.

At a higher level, COBIT has a set of 34 objectives, one for each of the IT processes. These processes are grouped under four domains. The domains and their respective control objectives are:

(a) **Planning and organization**

- Defining a strategic IT plan
- Defining the information architecture
- Determining the technological direction
- Defining the IT organization and relationships
- Managing the IT investments
- Communicating management aims and direction to stakeholders
- Managing human resources
- Ensuring compliance with external requirements
- Assessing risks
- Managing projects
- Managing quality

34 *Information System Audit and Assurance*

(b) Acquisition and implementation

- Identifying the solutions
- Acquiring and maintaining application software
- Acquiring and maintaining technology architecture
- Developing and maintaining IT procedures
- Installing and accrediting systems
- Managing changes

(c) Delivery and support

- Defining service level
- Managing third party service
- Managing performance and capacity
- Ensuring continuous service
- Ensuring system's security
- Identifying and attributing costs
- Educating and training users
- Assisting and advising IT customers
- Managing the configurations
- Managing problems and incidents
- Managing data
- Managing facilities
- Managing operations

(d) Monitoring

- Monitoring the processes
- Assessing internal control adequacy
- Obtaining independent assurance
- Providing for independent audit

For each of the 34 IT processes of the framework, there are from three to 30 detailed control objectives, totaling 318. In essence, the means by which these control objectives are addressed in an organization is called internal control. The next section will deal in detail with internal control, its objectives and issues related to its implementation.

INTERNAL CONTROL

The basic purpose of internal control in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented or

detected and corrected. This is achieved by designing an effective internal control framework, which comprises policies, procedures, practices, and organizational structure that gives reasonable assurances that the business objectives will be achieved. Ultimately all these policies, procedures, etc. are broken into discrete activities and supporting processes, which can be either manual or automated. Although the implementation of control in the manual and automated processes differ, its essence remains the same. Another aspect, which should be considered while implementing control is that it is not solely a procedure or policy which is performed at a certain point of time. It is on the contrary, an ongoing activity, based on risk assessment of the organization. The role of auditors is very important in evaluating the strength of control. Elements of control that should be considered when evaluating control strength include the nature of controls, i.e. whether they are preventive or detective, manual or programmed, and formal (documented) or ad hoc.

PREVENTIVE CONTROL

Preventive controls are those inputs, which are designed to protect the organization from unlawful activities. These attempt to predict the potential problems before they occur and make necessary adjustments. The broad characteristics of preventive controls are:

- (i) A clear cut understanding about the vulnerabilities of the asset
- (ii) Understanding probable threats
- (iii) Provision of necessary controls for probable threats from materializing

As has been discussed earlier in this chapter, any control can be implemented in both a manual and computerized environment for the same purpose. Only, the implementation methodology may differ from one environment to the other. Now let us discuss the examples of preventive controls and how the same control is implemented in different environments.

Examples

- Employ qualified personnel
- Segregation of duties
- Access control
- Vaccination against diseases
- Documentation

36 *Information System Audit and Assurance*

- Prescribing appropriate books for a course
- Training and retraining of staff
- Authorization of transactions
- Validation, edit checks in the application
- Firewalls
- Anti-virus software (sometimes this acts like a corrective control also), etc.
- Passwords

The examples given above are in no way exhaustive, but are a mix of manual and computerized, preventive controls. Now let us see how the same purpose is achieved by using manual and computerized controls.

Table 2.1 Preventive controls

<i>Purpose</i>	<i>Manual Control</i>	<i>Computerized Control</i>
Restrict unauthorized entry into the premises	Build a gate and post a security guard	Use access control software, smartcard, biometrics, etc.
Restrict unauthorized entry into the software applications	Keep the computer in a secured location and allow only authorized persons to use the applications	Use access control, viz. user ID, password, smartcard, etc.

DETECTIVE CONTROL

Detective controls are those which detect and report the occurrences of an error, omission or malicious act in the Information System. The main characteristics of such controls are as follows:

- Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.
- An established mechanism to refer the reported unlawful activities to the appropriate person or group
- Interaction with the preventive control to prevent such acts from occurring

Examples of Detective Controls

- Surprise checks by supervisor
- Hash totals
- Check points in production jobs
- Echo control in telecommunications
- Error message over tape labels
- Duplicate checking of calculations
- Periodic performance reporting with variances
- Past-due accounts report
- The internal audit functions
- Intrusion detection system
- Cash counts and bank reconciliation
- Monitoring expenditures against budgeted amount

CORRECTIVE CONTROL

Corrective controls are very important because prevention and detection alone cannot be effective unless there is an appropriate corrective mechanism in place. The main characteristics of the corrective controls are:

- Minimize the impact of the threat
- Identify the cause of the problem
- Remedy problems discovered by detective controls
- Get feedback from preventive and detective controls
- Correct error arising from a problem
- Modify the processing systems to minimize future occurrences of the problem

Examples of Corrective Controls

- Contingency planning
- Backup procedure
- Rerun procedures
- Treatment procedures for a disease
- Change input value to an application system
- Investigate budget variance and report violations

COMPENSATORY CONTROL

Controls are basically designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause a loss to that asset. While designing the appropriate control one thing should be kept in mind— *the cost of the lock should not be more than the cost of the assets it protects*. Sometimes while designing and implementing controls, organizations because of different constraints like financial, administrative or operational, may not be able to implement appropriate controls. In such a scenario, there should be adequate compensatory measures which may although not be as efficient as the appropriate control, can indubitably reduce the probability of threats to the assets. Such measures are called compensatory controls. Some examples of compensatory control given below will make the concept more clear.

Box 2.2

A data center needs a biometric access system, but the management feels that implementing biometric control to regulate entry of people in the data center will be too costly for them. Therefore, they decide to employ some compensatory controls like engaging a full-time security guard who is instructed to allow only those people into the center who have with appropriate access cards and to maintain a register for entering the access details, which will be supervised by the security officer. Such controls are compensatory in nature.

Let us take another example that involves implementing a strict segregation of duties as prescribed by ISACA (Information System Audit Control Association). In smaller information-processing environments, adequate segregation of duties between operation and programming may not be achievable. In these situations, it is important that compensating controls, such as strong computer security and end user reconciliation of control reports are implemented.

Another example could be the guidelines of the Reserve Bank of India which requires banks to segregate the three areas of Information Security, IS Audit and Information Technology to avoid a possible role clash and to ensure independence of each area. Although creating these three separate departments could help in appropriate control of bank's operations, this may not be feasible in many public sector banks due to cost constraints. The compensatory controls that can be employed instead can include making IT audit a part of the existing Audit and Inspection department and creating a separate group of IT security within the Information Technology department, with little change in the reporting structure. For instance, the head of IT security can directly report to the head of IT.

INFORMATION SYSTEM CONTROL PROCEDURES

General IT controls apply to all functions within an organization. Control procedures include policies and practices established by the management to provide reasonable assurance that the specific objectives of the organization will be achieved.

Examples of General Control Procedures

- Strategy and direction
- General organization and management
- Access to data and programs
- Systems development and change control
- Data processing operations
- System programming and technical support functions
- Quality assurance procedures
- Physical access controls
- Business continuity/ disaster recovery planning
- Network and communications
- Database administration

Each general control procedure can be translated into Information System-specific procedures and applied to the Information System. What is important to remember here, is that a person who is good with general controls or a person who is aware about the working of controls in a manual environment can effectively prescribe controls for an IT environment. Translating general controls to IT controls for implementation purposes, requires the knowledge of Information Technology.

Let us take the example of a legacy bank in India going for a core banking solution. In this case, the officials who are conversant with the controls in the manual environment should be associated with the core banking project to evaluate the appropriate controls in an IT environment.

Information control procedures can be categorized into the following areas:

- General organization control procedures
- Access to data and programs
- System development methodologies
- Data processing operations
- System programming and technical support functions
- Data processing quality-assurance procedures

Box 2.3**Baring loses \$1 billion due to lack of internal controls**

On February 23, 1995, a 232 year-old British bank, Baring Bros. and Co., went bankrupt due to a loss of \$1 billion in futures trading by an employee, Nick Leeson. A statement by the Singapore International Monetary Exchange (SIMEX) attributed the loss to a *failure of internal controls*. [Associated Press, March 5, 1995]. Senior executives conceded that controls should have been much tighter. The organization ignored several warning signs of internal control weaknesses over several years:

- In *March 1992*, a senior executive in Singapore wrote a letter to the head of the equity department in London stating, "My concern is that once again we are in danger of setting up a structure which will subsequently prove disastrous and with which we will succeed in losing either a lot of money or client goodwill or probably both. In my view, it is critical that we should keep clear reporting lines and if this office is involved in SIMEX at all then [Mr Lesson] should report to the Singapore office operations department not the London derivatives department."
- An internal audit report in the summer of 1994, cited lax internal controls and made a specific recommendation that the trading and settlement duties be separated. Mr Lesson at the time was in charge of both duties.
- Mr Lesson used an error account to hide trades that he did not want his superiors to know about.

Managers were reluctant to impose tight controls, which might have reduced profits and bonuses.

Source: Brauchli, Marcus W., Bray, Nicholas, and Sesit, Michael, "Barings PLC Officials May Have Been Aware of Trading Position," (1995) *Wall Street Journal*, March 6, 1995, p. 1, 6.

INTERNAL CONTROL AND INFORMATION SYSTEM AUDIT

The overall purpose of controls is to reduce chances of the unexpected losses from unlawful events that can occur in the system. These unlawful events can take place if unauthorized, inaccurate, incomplete, redundant, ineffective or inefficient inputs enter the system. The auditor's task is to determine whether the appropriate controls are in place and working effectively to prevent, detect, and correct such unlawful activities. The following points are to be taken care of by the auditors while evaluating controls.

Audit Risk and Materiality

Materiality can be understood in the context of how significant a loss is to the organization if a particular control is absent, ineffective or inefficient. For judging materiality, the auditor should first acquire an understanding of the nature of the business, inherent risks and the extent of likely loss to the core activities of the organization. Since evaluating the materiality of the risk for an organization involves subjectivity, it may happen that the auditor fails to detect actual or potential material losses. The probability of an auditor failing to detect the material loss is called audit risk. These audit risks are categorized below.

Inherent Risk

Inherent risks are independent of audit and can occur because of the nature of the business. Since inherent risks are constant and exist before the reliability of the control is considered, auditors should juxtapose other existing risks having no compensatory control with the inherent risk for finding out the materiality. For example, the risk of not posting a security guard in front of a vault containing a lot of cash is considered more material than not posting a security guard to protect an inventory of coal.

Control Risk

Control risk is basically the gap between the desired and existing risk. It must be noted that this gap may result in material loss to the organization.

Detection Risk

Detection risks are those that remain undetected by the auditors. This could be because of inadequate test procedures, lack of appropriate domain knowledge of the auditors, etc. Intentional non-detection by the auditor cannot be considered as a detection risk.

As a basis of determining the level of desired audit risk, some professional bodies of auditors like the American Institute of Certified Public Accountant (AICPA), have adopted the following audit risk model for the external audit function:

$$DAR = IR \times CR \times DR$$

DAR = Desired Audit Risk

IR = Inherent Risk

CR = Control Risk

DR = Detection Risk

Audit Procedures for Evaluating Control

The following procedures are generally followed by auditors for evaluating controls:

I. Gathering Information and Planning

This is basically the pre-evaluation phase where auditors gather knowledge of the business and industry and determine the inherent risks, the regulatory statutes pertaining to the organization. The previous year's audit result also needs to be considered at this stage. For a typical Information System Audit of a bank for instance, the balance sheets of the last two to three years and the IT plan would be the necessary documents, required at this stage. For external auditors, this step may not necessarily be performed onsite.

II. Understanding Internal Control

Inquiries, inspection, and observation can be used to gain an understanding of the controls that supposedly exist, how well they have been designed and whether they have been placed in operation. For an Information System Audit of a bank, the auditor can have a customized questionnaire designed, which can be administered to officials at different levels. The following documents should be analyzed to assess the existing control environment:

- Information System security policy
- Information System security procedures
- User and system manual for different applications
- Job cards, etc.

At this stage, the auditors should conduct control risk and detection risk assessment, and calculate total risk.

One might ask what would happen if the documents mentioned above are not available with the bank (organization)? In such a situation, the auditors should map existing practices in the organization with best practices in the industries and business standards like BS7799 and COBIT and find the control gap.

III. Test of Control

Having identified the controls, the next step is to test whether these are acting effectively or not. It is not necessary that there should be automated procedures to test controls. This can even be done through inspection, observation, etc. These kinds of evidence gathering procedures, which could be manual or

automated and that are aimed at testing an organization's compliance with control procedures, are called *compliance testing procedures*.

A compliance test determines if controls are being applied in a manner that complies with management policies and procedures. For example, if the IS auditor is concerned about whether the program library controls are working properly or not, the IS auditor might select a sample of programs to determine if their source and object version are the same. Inspecting the firewall rule set and comparing this with the change control procedures is also an example of compliance testing.

IV. Substantive Test of Detailed Transactions

Evidence gathering for the purpose of evaluating the integrity of individual transaction, data or other information is called *substantive testing*.

An IS auditor uses substantive tests to check for monetary errors, directly affecting financial statement balances. A test for ensuring that the income tax calculation is in accordance with the existing income tax rule is an example of substantive testing. To perform substantive testing, the IS auditor might take the entire population or use a statistical sampling (discussed later in this chapter).

If the auditor finds that although there are some control practices, there are no documented policies and procedures, then he/she is likely to conduct more substantive tests. This will also happen in cases where the compliance tests are not satisfactory.

V. Analytical Review Procedures

Analytical procedures focus on the relationship between various data items, with the objective of identifying areas that require further audit work.

AUDIT EVIDENCE

Evidence gathering and evaluation is one of the fundamental tasks for the auditor who has to give an unqualified opinion about the state of the Information System.

Types of Audit Evidence

Audit evidence not only includes physical items, but also the observations of the IS auditors notes taken during interviews, internal correspondences, test results, etc. While all the evidence is meant for helping the auditors reach an

44 *Information System Audit and Assurance*

audit conclusion, the following attributes of the evidence should be considered by the auditors before evaluating the evidence.

Independence of the Provider

Evidence provided by a third party or any person/entity, independent of both the auditor and the auditee is considered more reliable than evidence provided by internal sources.

Qualification of the Evidence Provider

This is very important from the Information System's point of view, as the person providing the evidence should be able to understand its application. This also holds good for the test result conducted by a qualified/experienced auditor, which is considered more reliable than the test conducted by an incompetent auditor.

Objectivity of the Evidence

Objective evidence is considered more reliable than subjective evidence. For example, analyzing the system down time from a down time register would be more reliable than obtaining evidence of system down time through interaction and interviews with the system personnel.

Availability of Audit Evidence

IS auditors should choose the appropriate time and place for finding the relevant evidence. For example, when audit evidence is processed by Electronic Data Interchange (EDI), spread sheets may not be retrievable after a specified period of time if the changes made to the files are not controlled or the files are not backed up.

SAMPLING

Sampling, one of the major statistical techniques is gradually making its presence felt in IS auditing. An IS auditor should follow a methodological approach to reap the maximum benefits that the sampling technique has to offer. The present discussion attempts to provide a conceptual understanding of sampling and its methodologies. The discussion starts with a brief account of sampling.

The concept of 'population' is the key to sampling and its understanding is therefore, essential. A population can be designated as '*a collection of all the*

data points being studied'. The subset of a population can be defined as a sample. For instance, an IS auditor has to verify the records of all the employees in an organization. In this case, the records of a particular department, particular age group, particular designation, etc., will become the samples of the given population.

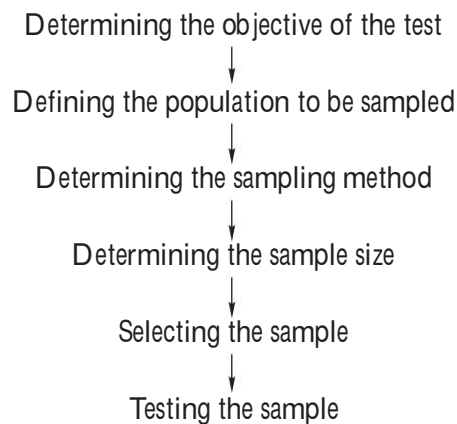
Advantages of Sampling

Readers may raise a very fundamental question— why should an IS auditor undertake a sample study instead of a population study? This is because sampling offers the following benefits vis-a-vis a population study:

- Studying a sample is more economical than studying an entire population
- Sampling provides quicker information to the IS auditor
- Sampling involves lesser work than that involved in studying the entire population. So, the chances of errors in data processing are lesser in the case of a sample study

Steps in the Construction and Selection of a Sample

The following six steps are essential to construct and select a sample for an IS audit:



- Here the first step, i.e. determining the objective of the test, depends upon the objective of the audit. Based upon the objective of the test, sample size, selection, etc., will be decided.
- The second step is defining the population to be sampled. As we discussed earlier, the population is the entire set of data from which

the IS auditor wishes to draw out a sample, in order to arrive at a conclusion. Hence, the population chosen from which the sample has to be drawn, should be appropriate and in line with the overall audit objective. While designing the sample, the IS auditor should ensure that the elements of the sample represent the characteristics of entire population.

- The third step is determining the sampling method. Based upon the methodology used, there exist different sampling approaches. In order to select a method of sampling, an IS auditor initially has to select an approach, method, and model for sampling. Each of these methods is discussed briefly in the forthcoming sections.
- The fourth step is determining the sample size. Sample size refers to the number of data members to be incorporated into a sample. While deciding the sample size, an IS auditor should consider following five factors:

Expected Error Rate

It can be designated as an estimate, stated as a percent of the errors that may exist. As no estimation inferred from a sample can be perfect, the IS auditor should attach an expected error rate to the sample.

Amount of Variability

It represents the range of values in the population that will affect the accuracy of the estimate and in turn the sample size. The more the variability, the less accurate the estimate and hence a larger sample size will be required.

Confidence Level

It can be designated as the probability that the characteristics of the sample are a true representation of the population. The larger the sample size, the higher will be the confidence level.

Population Size

The final factor is population size. The larger the population size, the larger will be the sample size, as the sample has to represent most of the features of the population.

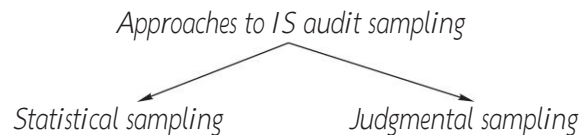
While determining the sample size, the IS auditor should consider the sampling risks, the amount of errors that are acceptable and the extent to which errors are expected. It can be designated as the probability that the

characteristics of a sample are not a true representation of the entire population. Mathematically, it is equivalent to 1 minus the confidence coefficient. Apart from this, to be able to effectively conduct risk assessment, the IS auditor should be conversant with concepts of *population standard deviation* and *sample standard deviation*. While population standard deviation refers to the distance between the population mean and each item in the population, sample standard deviation refers to the distance between the sample mean and each item in the sample.

- The fifth step is selection of the sample. Different methods exist to select a sample. Each of these methods is discussed in brief in the forthcoming sections.
- The final step is testing the sample.

Approaches to Audit Sampling

Broadly, approaches to audit sampling can be classified as follows:



Statistical Sampling

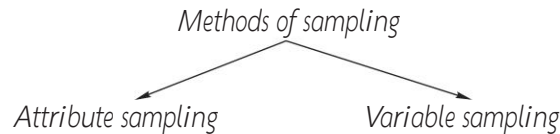
In this approach, the IS auditor mathematically/statistically decides the sample size, its method of selection and the confidence level. In this approach, generally, the analysis and results are based upon quantitative values.

Judgmental Sampling

In this approach, instead of statistical analysis, the IS auditor depends upon his/her own judgmental analysis to estimate the sample size, its method of selection, and the confidence level. Generally, judgmental analysis depends upon the level of materiality and risk of each data member in the set. Judgmental sampling allows the IS auditor to test a chosen portion of the entire population. In this approach, even though the IS auditor cannot statistically relate the results of the selected sample to the entire population, he/she can identify specific exceptions in the sample and further, can comment on the root causes of these exceptions.

Methods of Sampling

Each of the approaches discussed above can be conducted with the following two methods of sampling:



Attribute Sampling

It is useful in determining the attributes of a population. The results of such a sampling test are generally expressed as a percentage of the type of event specified. It is generally used when the question of 'how many?' arises. Attribute sampling can be achieved with the help of the following three sampling models:

Frequency Estimating Sampling

In this model, the IS auditor estimates the proportion of items in a population containing a particular attribute of interest. Generally, this model is used for testing of controls of transactions.

Stop-or-Go Sampling

This model is used when the IS auditor requires to reach a conclusion about the upper precision limit of an attribute sample. It is used when the IS auditor believes that the chance of errors in a population will be low.

Discovery Sampling

It is also referred to as exploratory sampling. It is useful when evidence of a single error calls for a detailed audit. It is widely used in cases of fraud detection, avoidance of internal controls, etc.

Variable Sampling

Variable sampling or dollar estimation or mean estimation sampling refers to a technique that is used to estimate the value of a measure like the dollar or some other estimate like weight of the population, by estimating the population's measure. It is useful to answer the question, 'how much?'. It can be achieved through the following three models:

Stratified Mean Per Unit

In this model, based upon certain criteria, the entire population is subdivided into small groups or stratas and samples are drawn from each of these. This model is useful when a smaller sample size is required.

Unstratified Mean Per Unit

In this model, in order to project an estimated total, a sample mean is calculated. Here, sample mean refers to an arithmetic average of set observations in a sample.

Difference Estimation

This model can be used to estimate the difference between the book values and audited values.

Finally, an IS auditor cannot rely exclusively on statistical measures and completely ignore his/her commonsense. Ultimately, commonsense is what determines whether a decision maker will be successful or not.

COMPUTER ASSISTED AUDIT TOOLS AND TECHNIQUES (CAATTs)

For evaluation of controls in the Information System, auditors sometimes use some tools which are used in the computer system, an exercise also known as *auditing with the computer*, for extracting and evaluating evidence/ data. Such tools are basically data-mining tools and generically called Computer Assisted Audit Tools and Techniques (CAATTs). The development of CAATTs represents one of the most significant advances in technology, affecting the audit profession. The earlier black box approach of computer audit which is generally known as *auditing around the computer*, wherein the auditor only evaluated the output of the computer operations i.e. reports, etc. for arriving at the audit conclusion, is no more relevant in today's more complex Information Systems.

Use of CAATTs can significantly improve efficiency and effectiveness during the conduct of the audit and ensure consistent results. Tasks, which are impossible or too time consuming for the auditors to be performed manually, can be undertaken with the help of CAATTs. The computer is used for searching, sorting, matching, and performing various types of tests and mathematical calculations on the data. CAATTs is a combination of various tools and techniques.

Tools are those software packages, which are used for extracting, sorting, selecting the data and/or transactions from the database. However, the auditor

has to use his/her judgment while auditing the transactions to identify the discrepancies.

Techniques are the methods embedded in the software, which help auditors in collecting the evidence for audit.

Types of CAATTs

Packaged Software

Packaged softwares like MS Office, Lotus smart suite can also be regarded as CAATTs to a limited extent as they can be used by the auditors to extract data from various sources. Also the analysis can be done by the auditor, either by using the existing utilities in these applications or writing some customized macros.

Generalized Audit Software (GAS)

GAS comes in a variety of forms. It may either be a software package available commercially or one developed by an auditing firm. In most cases, the purpose of the software package is to interrogate the database on computer and extract information. This type of software may be used to gather evidence in relation to both the effectiveness of operation of a programmed control procedure and to know the extent of misstatements in account balances and underlying classes of transactions. In other words, this software may be used as either a test of control or a substantive procedure. Normally, GAS also provides utility to the auditor to develop customized utility using some scripts. In such a case, auditors need to have some programming skills. In any case auditors need some training to operate and use the GAS effectively.

Embedded Audit Module (EAM)

This is a technique in which the code prepared (recommended) by the auditor is embedded in the application software. The code may be designed, for example, to replicate a specific aspect of a control procedure or to record details of certain transactions in a file, accessible only to the auditor. Thus, it may be used as both a test of control and a substantive procedure. However, it may not be possible to embed audit module after the software is developed and implemented. A log parser built into the system and designed to send specific input to the auditor is an example of EAM.

Audit Hook (AH)

AH is the software module embedded in the application software, which selects the specific transactions from live data, while in process, for the audit. The criteria for selection of these transactions is provided by the auditor. This means that an EAM with parameterization left to the auditor is called Audit Hook.

Integrated Test Facility (ITF)

ITF is a facility, forming part of the application software that enables the auditor's test data to be integrated with the live data and to be then processed using the current production version of the software. The facility ensures that the test data updates special dummy files, rather than actual operating files. The dummy files are examined to ensure that the test data has been processed in the desired manner. This procedure provides evidence of the effectiveness of design of programmed control procedures. This however, does not help auditors in finding the transactional discrepancies within the acceptable control framework. It only provides the assurance that the controls designed in the software are working as expected. It does not perform the task of auditing transactions.

Parallel Simulation (PS)

PS is a process in which live data is processed using the auditor's copy of the software. The data, processed on the copy of the software is compared with the data previously processed in live environment to ensure that the processing is identical. This procedure provides evidence of the effectiveness of the design of the programmed control procedures.

Program Code Analysis (PCA)

PCA is the analysis of the application program code, which is done to ensure that the instructions given to the computer are the same as issued by the auditor when reviewing the systems documentation. The analysis may be performed using Specialized Audit Software (see next page), used by the auditor. The procedure provides evidence of the effectiveness of the design of the programmed control procedures.

Test Data

Test Data is a CAAT in which test data, prepared by the auditor, is processed on the current production version of the application software, but separately

from the normal production area. The test data that is processed, updates the auditor's copies of the original data files. The updated files are then examined to ensure that the transactions were processed in the manner desired. This procedure is typically used to gather evidence of the effectiveness of the design of the programmed control procedures.

Specialized Audit Software (SAS)

Specialized Audit Software is a software, designed to perform specific tasks in specific circumstances, such as comparison of source and object code, the analysis of unexecuted code and the generation of test data. It is used to gather evidence of the design effectiveness of application software. Specialized Audit Software can also be designed for specific application, customized for the organization.

Advantages of CAATTs

Greater Productivity through

- Reduced audit cycle; the periodicity of audits can be increased due to process automation
- Automated repetitive tasks which reduce the time required for audits and fatigue
- Focused effort and undivided time on critical functions
- Simplified project documentation due to automation
- Improved planning process; most CAATTs provide for proper planning of the audit process
- Eased report-writing process

Value Addition by

- Providing timely results; with less time gap between audits, irregularities can be reported and rectified much earlier
- Recuperating lost revenue; detailed analysis of 100% data can help find more income leakages
- Quantifying impact of given conditions
- Offering creative and detailed analysis of the Information System

Reducing Costs by

- Lowering EDP costs. Extra outputs for auditors are not required from the EDP department

- Minimizing software maintenance costs; most CAATTs can be customized easily, without writing or adding programs
- Reducing travel costs; auditors can perform audits without travel by using remote login and extracting data from live database

Improved Quality of Audits due to

- 100% audit of data files; CAATTs can analyze the entire data for a given audit period, thereby reducing the audit risk
- Standardized audit methodologies
- Verified audit procedures
- Assured integrity of analysis

Independence from Information Systems because of

- Simplified data access; with CAATTs there is no need to depend on technical persons to deliver the data/information
- Independent isolation of exceptions
- Elimination of the need to sample
- Elimination of the need to depend on the client's computer, to work

Reduce Audit Delivery Time

- Minimize wait-time required for getting information
- Accelerate the identification of exceptions
- Simplify the preparation of working papers; reports can be prepared by the automated process
- Automate the entire analysis; CAATTs can analyze data faster than manual operations

Corporate Benefits

- Reduce current risks; early detection of irregularities and frauds
- Help prepare for future risks; data analysis can indicate probable risk areas
- Recover audit investment by reducing audit cycle time and improving quality of audits
- More efficient
- More effective
- Help in optimal use of resources
- Bring about a real change in audit image

Personal Benefits to Auditor

- Independence
- Renewed focus on audit
- Elimination of repetitive work
- Greater creativity
- Reduced audit risk

Audit Benefits—Today's Technology

- Exception reporting
- Control analysis
- Statistical sampling
- Immediate results
- Easy to use: PC based
- Highly flexible
- Extremely fast
- Provide a lot more than just analysis

Disadvantages of CAATTs

- Training requirements for most of the CAATTs are extensive and therefore, can be cumbersome
- Even if the use of CAATTs is mastered, the techniques for selecting the transactions for audit will depend upon the auditor's creativity, experience, and understanding of the audit area
- Some CAATTs are so general that customizing them for specific use might be difficult
- Extracting the transaction data, in the format required by CAATTs for auditing, where the application is running across multiple platforms, might require high IT skills

Some Leading CAATTs

- ACL (Audit Command Language)– Data extraction and analysis software
- IDEA (Interactive Data Extraction and Analysis)– Data extraction and analysis software

- Audimation– The North American business partner for Caseware, IDEA provides software, training and support
- Audit Leverage– department management software for internal auditors; uses Microsoft access for workpapers, risk assessment, staffing and scheduling, timekeeping, and more
- Automated Audit Services– Links to articles, service, and training from a Win IDEA consultant
- Auto Audit 2001– Electronic workpapers software, allows auditors to compose risk assessments, audit schedules, plan documents, workpapers, review comments, audit reports, time reports, and expense reports, all with the help of a single database
- Galileo– Comprehensive and integrated audit management, documentation and reporting system for internal auditors and risk managers
- Magique– Integrated risk management system for organizations to quantify, assess, and control risks
- Pentana– Software for strategic audit planning, resource planning, actual time recording, automated audit checklists and programs, and action plan management
- TeamMate– Electronic work paper package that has revolutionized the audit documentation process

Selecting CAATT

Selection of CAATT depends on the requirements of the auditors, e.g. the internal audit department of an organization may develop the software for internal use or buy CAATT and customize only once. But the auditor who needs to audit clients' data, might require a software which can be used across multiple platforms.

However, some common considerations for selection of CAATTs are:

- Ease of use
- Capacity to handle the data
- Efficiency of analysis
- Level of training required
- Effectiveness in preventing and/or detecting frauds
- Cost and licensing structure
- Multi-user utility
- Platform independence

- Programming capability using customized script
- Security

'Internal Auditor', the magazine of the Institute of Internal Auditor, conducted a survey on the use of CAATTs by internal auditors in August 2001. The analysis of almost 7,900 responses from worldwide members of IIA showed the following results:

- The most common applications for these products include, selecting data samples for detailed analysis, testing entire populations for exceptions, analyzing results, finding exceptions, and detecting fraud
- Other uses include, financial ratio analysis and risk assessment
- The participants identified increased efficiency and effectiveness, as well as savings of both time and money, as the primary benefits of using the software

According to the survey, ACL is the most preferred audit software, among corporates and auditors as it provides various options for data extraction, analysis and reporting.

Use of CAATT in Banks

With the help of CAATT, various tasks of audit in bank branches, which are handled manually, can be automated. Illustrative areas that can be covered in the audit are:

- Interest earned on advances
- Interest paid on deposits
- Recovery of commission and income from non-fund business
- Scrutiny of large value transactions in cash credit accounts
- Transactions in dormant accounts

In case of interest paid/ received, results obtained after verification through CAATTs, can be compared with that charged by the bank and differences if any can be ascertained. It is also possible to ascertain whether interest has been recovered on all the loan accounts of the branch or not. Income leakage, which is an area of concern for banks, can be taken care of in this audit.

The most important advantage of automated audit is that it facilitates the audit of an entire population and ensures consistent results. It is possible to verify entire transactions that have occurred during a particular period of time or of all the loan/ deposit accounts in the branch, instead of restricting verification by test check, as is done in the case of manual audit.

Methodology

A fully automated audit program can be created, keeping in view the features of the database of the bank, application software used, and heads of account defined at the branch. Data for a particular period (say each quarter), can be called from the branch on a floppy, other media, or through the Internet as a mail attachment and can be analyzed through ACL or any other CAATs installed on a PC in the head office of the bank. Further, manual scrutiny may be required in respect of identified exceptions, which can be carried out at the branch.

CAATs are changing the way auditors perform their responsibilities, allowing them to complete their audits more efficiently and effectively. Audit software is being used to analyze large data files, identify anomalies, compare fields, perform queries, develop reports, and document audit steps. More importantly, tests performed with the aid of audit software can be performed on entire populations, rather than just samples. Internal auditors can report to the management on the basis of “100%” tests, thus giving the management a complete picture of the area in question. Given the increased emphasis on fraud detection, CAATs provide auditors with the flexibility to develop creative fraud detection procedures. For example, audit software may assist an auditor in comparing an accounts payable file, a payroll file, and a contractor file, to determine whether any current employees are being paid as contractors. Similarly, lists of vendor addresses can be compared with employee address files to see whether employees are paying invoices to companies that they own or operate. Finally, using CAATs can also allow auditors to play a consultative role, instructing clients on how to use CAATs for their own benefit.

STANDARDS OF INTERNAL CONTROL

Although standards and practices of internal control and corporate governance are still emerging, five documents issued by different agencies/organization are very important from the perspective of internal control framework and evaluation. These documents are: the Information Systems Audit and Control Foundation's '*COBIT Control Objectives for Information and related Technology*', the Institute of Internal Auditors Research Foundation's '*Systems Auditability and Control (SAC)*', the Committee of Sponsoring Organizations of the Treadway Commission's '*Internal Control—Integrated Framework (COSO)*', and the American Institute of Certified Public Accountants' '*Consideration of the Internal Control Structure in a Financial Statement Audit (SAS 55)*', as amended by Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55 (SAS 78).

Although a detailed discussion of all these standards is not in the scope of this book, a brief overview and a comparison among them could be useful for the readers.

COBIT (1996) is a framework providing a tool for business process owners to efficiently and effectively discharge their IS control responsibilities. SAC (1991, revised 1994) offers assistance to internal auditors on the control and audit of Information Systems and technology.

COSO (1992) makes recommendations to the management on how to evaluate, report, and improve control systems.

SASs 55 (1988b) and 78 (1995) provide guidance to external auditors regarding the impact of internal control on planning and performing an audit of an organization's financial statements.

As different bodies developed the documents to address the specific needs of their own audiences, some disparities may exist. Nevertheless, each document focuses on internal control and each audience, i.e., internal auditors, management, and external auditors, devotes much time and effort towards establishing or evaluating internal controls. Therefore, comparing the internal control concepts presented in these documents could be of interest to the readers.

A comparison of the five documents reveals that each builds on the contributions of the previous documents. COBIT incorporates as part of its source documents both COSO and SAC. It takes its definition of control from COSO and its definition of IT control objectives from SAC. SAC embodies the internal control concepts developed in SAS 55, COSO uses the internal control concepts in both SAS 55 and SAC, and SAS 78 amends SAS 55 to reflect the contributions to internal control concepts made by COSO.

Table 2.2 summarizes the four documents (Note: SAC 55/78 are combined).

INTERNAL CONTROL FRAMEWORK FOR BANKING SECTOR

The Risk Management Committee on Basle Committee of Banking Supervision, released a document in September 1998 titled "Framework for Internal Control System in banking organization". This document provides thirteen (13) principles grouped under six (6) major heads, viz.:

- Management oversight and the board control culture
- Risk recognition and assessment
- Control activities and segregation of duties

Table 2.2 Comparison of various standards of internal control

	COBIT	SAC	COSO	SAS 55/78
Primary audience	Management, users, Information System auditors	Internal auditors	Management	External auditors
Internal control viewed as	Set of processes including policies, procedures, practices, and organizational structures	Set of processes, subsystems, and people	Process	Process
Internal control objectives	Effective and efficient operations confidentiality, integrity and availability of information, reliable financial reporting, compliance with laws	Effective and efficient operations, reliable financial reporting, compliance with laws	Effective and efficient operations, reliable financial reporting, compliance with laws	Reliable financial reporting effective and efficient operations, compliance with laws
Components or domains	Domains: Planning and organization, acquisition and implementation, delivery and support, monitoring	Components: Control environment, manual and automated systems control procedures	Components: Control environment, risk management, control activities, information and communication monitoring	Components: Control environment, risk assessment, control activities, information and communication monitoring
Focus	Information Technology	Information Technology	Overall entity	Financial statement

(Contd)

	COBIT	SAC	COSO	SASs 55/78
Internal control effectiveness evaluated	For a specific period of time	For a period of time	At a point in time	For a period of time
Responsibility for internal control system	Management	Management	Management	Management
Size	187 pages in four documents	1193 pages in 12 modules	353 pages in four volumes	63 pages in two documents

- Information and communications
- Monitoring activities and correcting deficiencies
- Evaluation of internal control systems by supervising authorities

The details of this document can be accessed from the Bank of International Settlement's (BIS) website www.bis.org

SUMMARY

In this chapter we discussed the fundamental concepts of control and how it evolved from the definition prescribed in the control theory for high-level systems to the controls prescribed by ISACA and also by COBIT. We inferred that the essence of control has not changed over the years and it will continue to remain unaltered in future. The implementation of control may differ from a manual to an automated or Information Technology environment. We then discussed internal control, the types of internal control, i.e. preventive, detective, corrective, and compensatory control, with examples from both the manual and IT environment. The role of auditors in the evaluation of internal controls was also discussed at length, with special emphasis on materiality, audit evidence, use of CAATTs, etc. We also discussed the various internal control standards and undertook a comparative study of these. The document released by Basle Committee of Banking Supervision, viz. "Framework of Internal Control System in Banking Organization" was also discussed in brief at the end.

REVIEW QUESTIONS

1. What is control? Describe the evolution of control from the control theory for high-level systems to the control framework of COBIT.
2. Describe the control framework of COBIT.
3. What is internal control? Describe the various types of control, with examples.
4. What is compensatory control? Critically analyze the need for compensatory control in an organization.
5. Describe various Information System control procedures, with examples.
6. Describe the relationship of internal control with Information System Audit.
7. What is audit evidence? What are the important points that IS Auditors need to remember while for collecting and evaluating evidence.

8. Describe various sampling methods available to IS auditors.
9. What are Computer Assisted audit Tools and Techniques (CAATTs)? Describe the types of CAATTs and their usefulness to IS auditors.
10. Give a comparative analysis of various standards of internal control.
11. Write with examples, the differences between compliance and substantive testing.

MULTIPLE CHOICE QUESTIONS

1. Which of the statements below are not correct?
 - (a) Control is not required if the system is not dynamic
 - (b) If the dynamism of a system is predictable, then the control becomes less predictable
 - (c) The input should be based on desired output
 - (d) The output should be evaluated for giving further input to the system
2. Which of the following statements about control, is false?
 - (a) The primary focus of control is unlawful events
 - (b) Control is a system of interacting components
 - (c) Control covers all unlawful events in a system
 - (d) An unlawful event in a system can be covered by more than one control
3. Over which type of risk does the auditor have least control?
 - (a) Control risk
 - (b) Desired audit risk
 - (c) Detection risk
 - (d) Inherent risk
4. Training imparted to a group of officials of a bank in the area of Information System Audit is an example of:
 - (a) Preventive control
 - (b) Detective control
 - (c) Corrective control
 - (e) Traditional audit
5. In case the auditor finds that there are no documented controls in the organization, what step should he/she take?
 - (a) Immediately stop audit and wait for the documents to be prepared
 - (b) Inform the management

- (c) Evaluate the control process and map this to the existing industry good practices and find the gap.
- (d) Conduct more compliance testing
- 6. If the auditor does not want to rely on compliance testing, then he/she should:
 - (a) Do more interviews
 - (b) Use specialized audit software
 - (a) Conduct extensive substantive testing
 - (c) Report to the management
- 7. Under what circumstances will the level of achieved audit risk decrease?
 - (a) An increase in inherent risk
 - (b) A decrease in detection risk
 - (c) An increase in control risk
 - (d) A decrease in desired control
- 8. Embedded Audit Module (EAM) is a technique where:
 - (a) The code prepared (recommended) by the auditor is embedded in the application after the software is developed
 - (b) The auditor can use this as a substantive procedure
 - (c) A customized code as per the advice of the auditor is embedded in the application during the development process
 - (d) The auditor can parameterize the requirement at the application stage
- 9. Which of the following is true about Audit Hook (AH)?
 - (a) It is a specialized audit software
 - (b) It is EAM with parameterization left to the auditor
 - (c) It is used in a test environment
 - (d) It is used to compare data in a test environment with that of a live environment
- 10. Which of the following tests is an auditor performing when a sample of programs is selected to determine if the source and the object versions are the same?
 - (a) A substantive test of program library controls
 - (b) A compliance test of program library controls
 - (c) A compliance test of the program compiler control
 - (d) A substantive test of the program compiler controls

11. A member of the Board of Directors of your company, where you work as an IS Auditor has told you in confidence, about the forthcoming changes in the IT department. What should you do?
 - (a) Inform the IT manager about the impending changes since these are likely to his/her department
 - (b) Inform your manager about the forthcoming changes, since your these department will need to change the audit plan to accommodate these changes
 - (c) Not inform anybody, since it amounts to a breach of trust
 - (d) Inform both, the EDP manager and your manager, as the changes are going to affect both departments
12. The primary objective of test of controls is to:
 - (a) Determine whether controls are operating effectively
 - (b) Identify the material errors that have occurred in major classes of transactions
 - (c) Understand whether a control is in place
 - (d) Identify major patterns of errors or irregularities that might exist in final account balances
13. Which of the following is a compliance test?
 - (a) Preparing confirmation request using stratified random sampling
 - (b) Tracing a sample of credit invoices to transactional documents
 - (c) Aging the balances due by invoice
 - (d) Footing the accounts receivable file and reconciling it with control accounts
14. An IS auditor concerned that application controls are not adequate to prevent duplicate payment of invoices, decides to review the data processing files for possible duplicate payments. In the review, the IS auditor would most probably make use of:
 - (a) An integrated test facility
 - (b) Statistical sampling
 - (c) Generalized audit software
 - (d) The audit review file
15. Which of the following types of control would an IS auditor look for when a weakness in a system of control is discovered:
 - (a) Compensatory
 - (b) Preventive
 - (c) Corrective
 - (d) Detective

DISCUSSIONS AND RESEARCH QUESTIONS

1. A person who is conversant with the controls in a manual environment could be the appropriate person to be involved in the design process of automating the manual environment for suggesting the necessary control requirement. Discuss.
2. “Auditors are control advocates”. Discuss this in the context of the role of an auditor in internal control evaluation.
3. Computer Assisted Audit Tools and Techniques (CAATTs) are just data-mining tools. An auditor with excellent programming skill therefore, does not require any CAATT when auditing with the computer. Discuss.
4. Understanding the materiality of the loss to the organization is most important for the auditor. Discuss this in the context of risk based audit approach.

EXERCISES

1. Visit the websites of some major CAATTs mentioned in the chapter and describe the utilities they provide.
2. Map the internal control of your own organization with any of the standards described in the chapter.
3. Visit the website of Bank for International Settlement and critically discuss the document “Framework of Internal control system in Banking Organizations”.

CASE STUDY WHO CONTROLS BANKING?

Mr Sharma set aside the magazine he was reading and lazily looked out of the window. He was fascinated by the clouds, which looked like bundles of cotton with the sunrays reflecting brightly on them. “Really I am on cloud nine”, he thought happily, remembering how he had been promoted recently. He was on his way to take over as branch manager of the Santacruz, Mumbai branch of the People’s Comfort Bank. He dozed off, dreaming about his new assignment.

A sudden jolt woke him up from his slumber. The plane had landed. Outside the airport, the previous manager of the Santacruz branch, Mr Verma, who was also his friend, was waiting to take him home. It was a luxury, by

Mumbai standards, to have a flat right above the branch in the same building. “I can give maximum attention to the bank’s business activities now”, thought Mr Sharma. “I will make this branch the best in the country”, he said to himself, quietly. He then started discussing the current position of the branch with Mr Verma.

The branch had been totally computerized a year ago, although none of the employees had been formally trained in working with computers. “All the employees of the branch are very intelligent and they did not need any training”, Mr Verma said proudly. “HO was particularly happy with our branch for not incurring any expenditure on computer training for the employees. For any help required, the vendor’s support is always there”, he continued. Mr Verma was considerably familiar with technology and went ahead to describe that the Operating System used was Novell Netware 4.11 and that the data was specially stored in Btrieve files, which could not be accessed outside the system.

This made Mr Sharma feel quite uncomfortable, as he was not familiar with computer jargon. He was an excellent banker, but so far he had not worked in a computerized branch. The feeling of euphoria over taking charge as branch manager started to evaporate slowly. He suddenly remembered the article he had been reading on the plane. The caption of the article was “Who controls Banking?”, and it was concerned with the increasing dependence of banks on computer technology. The article had discussed the benefits and drawbacks of computerization of banking activity. One point that had caught the attention of Mr Sharma was that the author had emphasized the need for the bank management to ensure that technology is subservient to it and not the other way around.

With renewed hopes he asked his friend, “Surely, you have ways in which you can ensure that whatever goes on, is going on okay.” His friend laughed and said, “When computers are doing the job, there is no room for doubts. How can computers make mistakes? They have been programmed to do things right. I am a techno-savvy man, so I know this”. Mr Sharma nodded, but his common sense warned him that something was not quite okay with what Mr Verma had just stated. “Human intelligence cannot be underestimated. It is the duty of the management to see that the bank’s business goes on correctly,” he thought.

The first day in the branch was quite uneventful. Mr Sharma saw that the customers were a happy lot, as they got quick service compared to earlier times. Many came and congratulated him. General Ledger was stroke balanced. The second day, Mr Sharma ventured near the computer terminal in the server room to witness the day-end operation that was being done on the computer. Mr Verma was standing proudly nearby. The process of handing over the

charge to Mr Sharma was still underway. Mr Sharma was glancing at the closing balances flying past on the computer screen, when he noticed a star (*). He asked what that meant. “Oh, that’s okay”, said Mr Verma, “the program indicates a (*) against all the balances where there is a mismatch between the book closing balance and the one that is computed by applying the day’s transactions to the opening balance. These accounts need to be looked into and reconciled. But you see, who has the time? I have asked for additional hands to take up that exercise. You can get it done when they are posted. But God knows when that will happen!”

Mr Sharma casually asked the person, who he had seen in the server room, operating the terminal from day one, “When did you join the Bank?”, to which Mr Verma hurried to intercept, “Oh no, he is Mr Mehta from Banksoft Technologies, which has supplied us the software package. He helps our Assistant Manager, who is the Database Administrator (DBA). In fact, whenever there is any problem with the system, he logs in with the login ID and password of our DBA and resolves the problem. I rely on him totally. You can also do the same. He helps all the staff members, when they have problems with their computers.”

The next morning, Mr Verma introduced Mr Parekh, Director of Banksoft Technologies to Mr Sharma. “He is the new manager”, Mr Verma said. They shook hands. Mr Sharma asked him, “I have a small doubt. Is it possible for anyone to change the balance in any account?” To this Mr Parekh replied proudly, “Our software is foolproof. There is a parameter in the system named ‘Live run’. Till the time test runs are being done by the client, the value of this parameter will be set to ‘NO’ and manual corrections can be done to balances if things don’t work properly. The moment live run begins, the client is asked to set this parameter to ‘YES’. Thereafter, it will not be possible to change the balances. We have explained these things clearly in our manual. Come along, let me show you.”

All three were in for a surprise, when they checked the system and saw that the parameter value had been set to ‘NO’. Mr Verma sheepishly said, “I thought your man, Mr Mehta was taking care of all this.” Mr Sharma remembered the stars he had seen a while ago and he really started seeing stars. Mr Verma started to defend himself, “You see, Mr Mehta is really knowledgeable. He even knows hardware. For example, there was a hard disk crash last month, and he was the one who detected the problem, took the hard disk, replaced, it and even reloaded the entire system.” Mr Parekh maintained a business-like silence and soon bid farewell assuring the manager of his best services.

Soon, Mr Verma was relieved from his post and Mr Sharma took over. But his mind was not at rest. He spoke to his friends in other computerized branches. He learnt, there was something called Information Systems Audit which could study the computerised system and indicate the loopholes. He learnt that some other organizations, had something called an Information Security Policy which was a document outlining how the management could ensure the safeguarding of the information assets of the organization.

Meanwhile, a thought struck him and he called for information on accounts closed within the past one year. As he studied the transactions in some of these accounts, his worst fears were confirmed. Quick investigations revealed that a few of these were benami accounts and that plenty of money had been siphoned off, out of the branch by inflating the balances of some inoperative accounts and transferring the amounts to these new accounts by manipulations on the computer.

When Mr Sharma asked the DBA to load past transactions from backup tapes to investigate the matter further, the DBA informed that some of the tapes were not restoring data properly as they seemed damaged physically. The DBA then proceeded to look for the audit files that according to him would be on the hard disk for one year. However, it suddenly struck him that the disk had crashed recently and the system had been reloaded, resulting in deletion of the old audit files. When Mr Mehta was confronted with charges of defrauding the bank, he simply said that the DBA of the branch also used the same login ID and password as he, so there was an equal chance that he could have done it.

That night, Mr Sharma lay in bed, sleepless, wondering,

“What steps can I take immediately to improve the credibility of the computerized system?”

“What steps can I take in the long run to ensure that I have adequate control over the system?”

“What improvements in the internal control system are necessary so that such things will not recur?”

Disclaimer: All names of characters and companies occurring in this case study are fictitious. Any resemblance to existing entities is purely coincidental and unintentional.

3

Conducting Information System Audit

-
- ❖ Audit charter vs engagement letters
 - ❖ Audit planning
 - ❖ The risk assessment
 - ❖ Gap analysis
 - ❖ IS audit of a typical bank
-

Conducting Information System Audit is the ultimate activity an IS auditor or a prospective IS auditor would like to get associated with. Apart from the knowledge requirement for such an activity, there are some other prerequisites, which are very important for the auditors before they start conducting audit. In this chapter we will deliberate on those prerequisites and also discuss the methodologies for conducting IS Audit.

AUDIT CHARTER AND ENGAGEMENT LETTER

Audit charter refers to the document prepared by an organization for internal control and audit, which clearly states the management's responsibility, authority, and accountability for IS Audit exercise.

The words responsibility, authority, and accountability mentioned above are very important and should cover the following:

'Responsibility' should cover:

- (a) Mission statement
- (b) Aims/goals

70 *Information System Audit and Assurance*

- (c) Scope
- (d) Objectives
- (e) Independence
- (f) Relationship with external audit
- (g) Auditee's requirements
- (h) Critical success factors
- (i) Key performance indicators
- (j) Other measures of performance

'Authority' should cover:

- (a) Risk assessment
- (b) Right of access to information, personnel, locations, and systems, relevant to the performance of audit
- (c) Scope or any limitations of scope
- (d) Functions to be audited
- (e) Auditee's expectations
- (f) Organizational structure, including reporting lines to the board of directors/senior management/ designated authority
- (g) Gradation of IS Audit officials/staff

'Accountability' should cover:

- (a) Reporting lines to senior management/ board of directors/ designated authority
- (b) Assignment performance appraisals
- (c) Personnel performance appraisals
- (d) Staffing/ career development
- (e) Auditees' rights
- (f) Independent quality reviews
- (g) Assessment of compliance with standards
- (h) Benchmarking performance and functions
- (i) Assessment of completion of the audit plan
- (j) Comparison of budget with actual costs
- (k) Agreed actions, e.g. penalties when either party fails to carry out its responsibilities.

The audit charter forms a sound basis for communication with the auditee and should include references to the service level agreements for the following:

- (a) Availability for unplanned work
- (b) Delivery of reports
- (c) Costs
- (d) Response to auditee's complaints
- (e) Quality of service
- (f) Review of performance
- (g) Communication with the auditee
- (h) Needs assessment
- (i) Control risk self-assessment
- (j) Agreement on terms of reference for audit
- (k) Reporting process
- (l) Agreement on findings

The audit charter should be approved by the highest level of the management. In case of a bank, it should be approved by the board of directors or any board level sub-committee. It is not necessary to have an exclusive audit charter document. It can be part of the information security policy document of the bank. Once drawn up, the charter should not be changed frequently. There should also be an established change management procedure for making any changes to the audit charter.

Engagement letters are the audit charters for third-party auditors. Like the audit charter, this should also include objectives, and information on delegation of authority to the IS auditors. Engagement letters are issued by auditors to the management after the terms and conditions are agreed upon.

These are often used for individual assignments, setting out the scope and objectives of the relationship between the external IS audit agency and an organization. The following aspects should be considered while preparing an engagement letter for an IS auditor:

Under *responsibility*, the following should be addressed:

- (a) Scope
- (b) Objectives
- (c) Independence
- (d) Risk assessment
- (e) Specific auditee requirements
- (f) Deliverables

Under *authority*, the following should be addressed:

- (a) Right of access to information, personnel, locations, and systems relevant to the performance of the assignment
- (b) Scope or any limitations of scope
- (c) Documentary evidence/information of agreement on the terms and conditions of the engagement

Under *accountability*, the following should be addressed:

- (a) Designated/intended recipients of the reports
- (b) Auditees' rights
- (c) Quality reviews
- (d) Agreed completion dates
- (e) Agreed budgets/ fees, if available

A TYPICAL IS AUDIT CHARTER

Mission

The mission of the internal IS audit area is to provide independent and objective assurance, and consulting services, designed to add value and improve the organization's IS operations. It helps the organization accomplish its objectives by assuring that the Information System safeguards assets, maintains data integrity, fulfills the organizational goals effectively, and consumes resources efficiently.

Scope

At present the scope of the IS Audit is as under:

- Management control review
- Access control
- Application control review
- Database control
- Internet banking control
- Conversion audit
- Business continuity and disaster recovery

However, this is not a comprehensive list and the scope of IS audit can be altered as per the need of the organization.

IS Audit Structure

To ensure the independence of auditors and avoid a possible role conflict, IS audit should be part of the inspection and audit function and have a reporting line, different from the IT department.

Accountability

The chief audit executive, in the discharge of his/her duties, shall be accountable to the management (management level sub-committee) to:

- Provide an assessment of the adequacy and effectiveness of the organization's IT processes for controlling its activities and managing its risks in the areas set forth under 'mission' and 'scope' of work
- Report significant issues related to the processes for controlling the activities of the organization and its affiliates, including potential improvements to those processes, and provide information concerning such issues through a resolution
- Periodically provide information on the status and results of the annual IS audit plan and the sufficiency of IT department resources
- Coordinate with and provide supervision of other control and monitoring functions (risk management, compliance, security, legal, ethics, environmental, external audit) affecting the IT resources

Independence

To provide for the independence of internal IS audit, its personnel report to the chief audit executive/general manager, who reports functionally to the executive director and administratively to the board level sub-committee.

Responsibility

The chief audit executive and staff of the internal audit department have a responsibility to:

- Develop a flexible annual IS audit plan using an appropriate risk-based methodology, including any risks or control concerns identified by the management, and submit that plan to the board level sub-committee for review and approval as well as periodic updates

74 *Information System Audit and Assurance*

- Implement the annual audit plan, as approved, including as appropriate, any special tasks or projects requested by the management and audit committee
- Maintain a professional IS audit staff with sufficient knowledge, skills, experience, and professional certifications like CISA to meet the requirements of this charter
- Evaluate and assess significant merging/ consolidating functions and new or changing services, processes, operations, and control processes, coincident with their development, implementation, and/ or expansion
- Issue periodic reports to the appropriate committee and management, summarizing the results of audit activities
- Keep the audit management informed of emerging trends and successful practices in internal IS audit
- Provide a list of significant measurement goals and results to the audit management
- Assist in the investigation of significant, suspected, fraudulent activities within the organization and notify the management, and the audit management of the results
- Consider the scope of work of the external auditors and regulators, as appropriate, for the purpose of providing optimal audit coverage to the organization at a reasonable overall cost

Authority

The chief IS audit executive and staff of the internal IS audit department are authorized to:

- Have unrestricted access to all IS resources during the IS audit period, with proper change management procedures
- Conduct periodic penetration testing of the Internet infrastructure without affecting normal day to day operations
- Allocate resources, set frequencies, select subjects, determine scope of work, and apply the techniques required to accomplish audit objectives
- Obtain the necessary assistance of personnel in units of the organization where they perform IS audit, as well as other specialized services from within or outside the organization

The chief audit executive and staff of the internal IS audit department however, are not authorized to:

- Perform any operational duties for the organization or its affiliates
- Initiate or approve accounting transactions, external to the internal auditing department
- Direct the activities of any employee not employed by the internal IS Audit department, except to the extent that such employees have been appropriately assigned to IS audit teams or to otherwise assist the internal IS auditors

STANDARDS, PRACTICES AND GUIDELINES

The internal IS audit area is expected to meet or exceed the Standards for the Professional Practice of Internal IS Auditing, set by ISACA and also abide by the guidelines of regulators, and the laws of the country, pertaining to the profession.

Box 3.1

IS Auditing Standards

Issued by Information Systems Audit and Control Association (ISACA)

010 Audit charter

010.010 Responsibility, authority and accountability

The responsibility, authority and accountability of the Information Systems Audit function are to be appropriately documented in an audit charter or engagement letter.

020 Independence

020.010 Professional independence

In all matters related to auditing, the Information Systems auditor is to be independent of the auditee in attitude and appearance.

020.020 Organizational relationship

The Information Systems Audit function is to be sufficiently independent of the area being audited to permit objective completion of the audit.

030 Professional ethics and standards

030.010 Code of professional ethics

The Information Systems auditor is to adhere to the *Code of Professional Ethics* of the Information Systems Audit and Control Association.

(Contd)

030.020 Due professional care

Due professional care and observance of applicable professional auditing standards are to be exercised in all aspects of the Information Systems auditor's work.

040 Competence

040.010 Skills and knowledge

The Information Systems auditor is to be technically competent, having the skills and knowledge, necessary to perform the auditor's work.

040.020 Continuing professional education

The Information Systems auditor is to maintain technical competence through appropriate continuing professional education.

050 Planning

050.010 Audit planning

The Information Systems auditor is to plan the Information Systems Audit work to address the audit objectives and to comply with applicable professional auditing standards.

060 Performance of audit work

060.010 Supervision

Information Systems Audit staff are to be appropriately supervised to provide assurance that audit objectives are accomplished and applicable professional auditing standards are met.

060.020 Evidence

During the course of the audit, the Information Systems auditor is to obtain sufficient, reliable, relevant, and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

070 Reporting

070.010 Report content and form

The Information Systems auditor is to provide a report, in an appropriate form, to intended recipients upon the completion of audit work.

The audit report is to state the scope, objectives, period of coverage, and the nature and extent of the audit work performed. The report is to identify the organization, the intended recipients, and any restrictions on circulation. The report is to state the findings, conclusions and recommendations and any reservations or qualifications that the auditor has with respect to the audit.

(Contd)

080 Follow-up activities

080.010 Follow-up

The Information Systems auditor is to request and evaluate appropriate information on previous relevant findings, conclusions, and recommendations to determine whether appropriate actions have been implemented in a timely manner.

Effective date

These standards are effective for all Information Systems Audits with periods of coverage beginning 25th July 1997.

(Standards for IS Auditing used by permission of Information System Audit and Control Association)

AUDIT PLANNING

Planning is a process of determining in advance what to do, when and how to do it and by whom. Audit planning involves the development of an overall strategy, based on the understanding of the auditee (organization) the environment in which it operates, the possible lines of enquiry, and the kinds of information that should be gathered for the identified areas of audit. Planning also optimizes the transfer of knowledge from one audit exercise to another, with minimal cost and disruption to the auditee.

Elements of Audit Planning

Each and every audit activity must be adequately planned. Planning the audit includes understanding the auditee, determining the audit objectives, the audit scope, timing, audit criteria, methodology to be used, and resources required. All audit plans must be written and documented for approval by the appropriate authorities.

The following elements/steps are necessary for effective audit planning:

- Understanding the auditee's organization
- Determining the audit objectives and scope
- Performing risk analysis
- Conducting an internal control review
- Setting the audit scope and objective
- Developing the audit approach or audit strategy

Understanding of the Auditee's Organization

The auditor should acquire knowledge and understanding of the organization and its operational activities, and the circumstances under which it is operating. This knowledge and understanding, helps in the identification of the line of audit enquiry, determination of audit areas and audit objectives. The steps an IS auditor could take to gain an understanding of the business include:

- Touring key organization facilities
- Reading IT plans
- Reviewing previous reports
- Interviewing key managers to understand the business issues

In case of an auditor, planning for the IS audit of a bank or its branch, the following information is required to be collected by the auditor at the planning stage:

- The IT strategy and plan
- The IT architecture, i.e. centralized or distributed
- Particulars of the software applications used by the bank, viz. the operating system, database management system, language, etc.
- HR profile related to IT area
- All other information, which will help the auditor minimize the audit time without diluting the effectiveness

Audit Objectives

The audit objective is the central objective, which a particular audit exercise is to accomplish. For example, objective in the audit of internet banking infrastructure of a bank would be to collect and evaluate the evidence in order to assure the management and also any third party like the Reserve Bank of India (central bank of the country) or the government that the infrastructure is as per the guidelines issued by regulator/government and the delivery channel, i.e., internet banking will in no way be a hindrance in fulfilling the business objectives of the bank and will also not hamper the interest of the stakeholders.

Audit Scope

Audit scope is the area to be covered by the audit activity. It is also the basis on which the audit is conducted. A clear determination and statement of the scope of audit, acts as a defence for the auditor in case of any misunderstanding or allegation that the auditor did or did not cover certain aspects of audit.

Audit scope is aimed at achieving the audit objectives. The scope of audit is mentioned in the audit communication as an indication of the extent of coverage.

Timing

Timing refers to the period to be covered in audit, commencement date of audit, how long it will take, and when the final report is expected, etc. Milestones and deadlines need to be specified.

Audit Methodology

Audit methodology means the methods and techniques used for performing audit procedures, gathering data, and documenting audit evidence as a basis for opinions and conclusions. For example, the methodology used in confirming the existence of inventories is observing physical count of inventory and inspection. A few of the methodologies used by auditors are:

- Inspection
- Observation
- Counting
- Inquiry
- Interviewing
- Confirmation
- Computation
- Reconciliation
- Analysis
- Testing
- Sampling

Audit Approaches

Audit approaches will vary from one auditor to the other and also across different assignments. Essentially, it all depends on the nature of the assignment, the knowledge of the auditor, and the specifications in the charter or engagement letter. Broadly, there are three approaches followed across the industry, viz.

- Auditing around the computer
- Auditing through the computer
- Auditing with the computer

Auditing around the Computer

In such kind of an audit approach, auditors treat the computer as a black box and rely on the output of the computer. The emphasis here is on checking the correctness of the output/ data/ documents, with reference to the input of a process, without going into the details of the process itself. In such cases, the auditors check the procedural controls rather than the computer or automated control. This kind of approach is suitable for low-risk, well-tested applications with simple logic and where the auditor does not need to have much computer knowledge to conduct the exercise.

Auditing through the Computer

In this approach, the auditors should have a fair knowledge about the hardware, system software, and above all the programming language in which the application is written. In such cases, the computer program and the data become important for the auditors, who will verify the program logic and also write specific codes to test the data for correctness. Although this approach is very effective, it is not always feasible for two reasons. First, there are risks involved in working with live data and application. Second, auditors often lack knowledge of various kind of technologies.

Auditing with the Computer

This is one of the most ideal approaches, where the auditors use various tools to extract the data from the auditee's computer system, into an independent environment. They then use various data-mining techniques to analyze the data for arriving at audit conclusions. In such cases, although the auditor need not be a programmer (unlike required in the earlier approach), he/she needs a fair amount of computer skills for using the tools and analyzing the data. Of course, the programming skills of the auditors are always an added advantage. Even in the case of using automated tools, known as CAATT (Computer Assisted Audit Tools and Techniques), an auditor having programming skill can write customized programs, using the scripting utilities in the tools.

Resources

Resources mean the money, time, number, and mix of audit staff that may be required to complete a particular audit task. A combination of size and sensitivity of the organization determine the resource requirements, the period of audit, the audit scope, and other such factors.

Advantage of Audit Planning

Audit planning is a continuous process that goes on throughout the audit exercise. A properly drawn-up audit plan helps in efficient and effective conduct of audit. Some of the main advantages of audit planning are given below:

- Audit planning helps in ensuring that adequate attention is devoted to important areas of audit. The auditor, while planning an audit, must ensure that all the important aspects are adequately covered. Otherwise, it will lead to some important aspects being overlooked or paid inadequate attention to
- Audit planning helps in identifying potential problems. While preparing an audit plan, the auditor can perceive likely problems, which may arise during the audit. This helps in devising a suitable action plan to overcome such problems
- Audit planning helps in ensuring that the audit work is completed expeditiously
- Taking various aspects into consideration, the auditor can plan his/her procedures in such a manner that audit can be completed on a timely basis, eliminating unproductive efforts
- Planning helps in utilizing the staff properly
- Planning helps the auditor in determining what audit procedures are to be performed in achieving the audit objectives
- Audit planning acts as a direction for auditors in planning, conducting, and reporting of an audit assignment

RISK ASSESSMENT

Risk assessment is a method of determining what kinds of controls are needed to protect an organization's Information Systems and resources not just adequately, but also cost-effectively.

The risk assessment process examines a set of five variables. First, what is one trying to protect, how much is it worth, and how much depends on it? Second, what could potentially threaten the asset? Third, what weakness exists that would allow the threat to materialize? Fourth, if the threat occurs, what kind of loss could one have? And, fifth, what controls can one put in place that would reduce the loss if a threat occurred, or eliminate the threat altogether?

The five variables are explained in detail, as under:

1. *Assets*– are whatever one is trying to protect. Assets can include databases, information, personnel, facilities, applications, computer hardware and software, and communications hardware and software.
2. *Threats*– are events that could happen at any time. Even the most impeccable security mechanism cannot eliminate the possibility of every threat, such as hurricanes, earthquakes or fraud. But one can mitigate the impact if a threat materializes, or reduce its likelihood of occurrence. Examples of threats include natural disasters, e.g., cold, storms, lightning, subsidence, as well as embezzlement, espionage, sabotage, loss of key personnel, and theft.
3. *Vulnerabilities*– are weaknesses in the organization that can create conditions, which would allow the threat to adversely affect the organization by for instance, triggering a loss. Examples of vulnerable areas include access control, administration, accountability, compliance, policy, operating procedures, and training.
4. *Losses*– loss categories include direct loss, disclosure losses, loss of data integrity, losses due to data modification, and losses due to delays and denials of service.
5. *Safeguards*– are security controls which, when put in place, can eliminate, or mitigate the impact caused by the occurrence of a threat. Examples of safeguards would include biometric controls such as retina scanning and the use of encryption, awareness programs, redundant power sources, audit trails, visitor controls, and electronic monitoring.

International Standard Organization (ISO), in its report “Guidelines for the Management of IT security” defined risk as under:

The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets. The impact or relative severity of the risk is proportional to business value of the loss/damage and the estimated frequency of the threat.

Risk Assessment Methodology

The risk assessment process includes gathering information about assets, finding sources of threat for data, conducting a survey to identify vulnerabilities, and then analyse the information, to see what combination of asset-threat-vulnerability could trigger off a material loss to the organization, and then decide what safeguards can be put in place to reduce or eliminate the potential loss. The risk analysis manager must evaluate thousands of different

combinations in order to write a comprehensive report. As per guidelines given by National Institute of Standards and Technology (NIST), Technology Administration, US Department of Commerce, the risk assessment methodology encompasses nine steps, viz.

1. System characterization
2. Threat identification
3. Vulnerability identification
4. Control analysis
5. Determination of likelihood
6. Impact analysis
7. Risk determination
8. Control recommendations
9. Result documentation

System Characterization

Identifying risks for an IT system, requires a keen understanding of the system's processing environment. The person or persons who conduct risk assessment must therefore, first collect system-related information, which is usually classified as follows:

- Hardware software system interfaces, e.g. internal and external connectivity
- Data and information
- Persons who support and use the IT system
- System mission (e.g. the processes performed by the IT system)
- System and data criticality (e.g. the system's value or importance to an organization)
- System and data sensitivity

Additional information related to the operational environment of the IT system and its data includes (but is not limited to) the following:

- The functional requirements of the IT system
- Users of the system, e.g. system users who provide technical support to the IT system, application users who use the IT system to perform business functions
- System security policies, governing the IT system (organizational policies, regulatory requirements, laws, industry practices)

- System security architecture
- Current network topology (e.g. network diagram)
- Information storage protection that safeguards system and data availability, integrity, and confidentiality
- Flow of information pertaining to the IT system (e.g. system interfaces, system input and output flowchart)
- Technical controls used for the IT system (e.g. built-in or add-on security product that supports identification and authentication, discretionary or mandatory or role-based access control, audit, residual information protection, encryption methods)
- Management controls used for the IT system (e.g. rules of behavior, security planning)
- Operational controls used for the IT system (e.g. personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as as privileged user access versus standard user access)
- Physical security environment of the IT system (e.g. facility security, data center policies)
- Environmental security, implemented for the IT system's processing environment (e.g. controls for humidity, water, power, pollution, temperature, and chemicals)

For a system that is in the initiation or design phase, system information can be derived from the design or requirements document. For an IT system under development, it is necessary to define key security rules and attributes for the future. System design documents and the system security plan can provide useful information about the security of an IT system that is in the process of development.

For an operational IT system, data about the IT system is collected in its production environment, including data on system configuration, connectivity, and documented and undocumented procedures and practices. Therefore, the system description can be based on the security provided by the underlying infrastructure or on future security plans for the IT system.

INFORMATION GATHERING TECHNIQUES

Any or a combination of the following techniques can be used in gathering information relevant to the IT system, within its operational boundary.

Questionnaire

To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls, planned or used for the IT system. This questionnaire should be distributed among the technical and non-technical management personnel who are designing or supporting the IT system. The questionnaire could also be used during on-site visits and interviews.

On-site Interviews

Interviews with the IT system, support and management personnel, can enable the risk assessment personnel to collect useful information about the IT system (e.g. how the system is operated and managed, etc.). On-site visits also allow the risk assessment personnel to observe and gather information about the physical, environmental, and operational security mechanisms of the IT system. For systems, still in the design phase, an on-site visit would be a face-to-face data-gathering exercise and could provide the opportunity to evaluate the physical environment in which the IT system will operate.

Document Review

Policy documents (e.g. legislative documentation, directives), system documentation (e.g. system user guide, system administrative manual, system design and requirement document, acquisition document), and security-related documentation (e.g. previous audit report, risk assessment report, system test results, system security plans, security policies), can provide useful information about the security controls used by and planned for the IT system. An organization's mission impact analysis or asset criticality assessment, provides information regarding system and data criticality and sensitivity.

Use of Automated Scanning Tool

Proactive technical methods can be used to efficiently collect system information. For example, a network-mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s).

Threat Identification

A threat is the potential for a particular threat-source to successfully exploit a particular vulnerability. Vulnerability is a weakness that can get triggered

accidentally or intentionally exploited. A threat source does not present a risk when there is no vulnerability that can be exploited. In determining the likelihood of a threat, one must consider threat sources, potential vulnerabilities, and existing controls.

Threat Source Identification

The goal of this step is to identify the potential threat sources and compile a statement, listing these potential threat sources that are likely to affect the IT system being evaluated.

A threat source may be defined as *'any circumstance or event with the potential to cause harm to an IT system'*. The common threat sources can be classified as natural, human, or environmental.

In assessing threat sources, it is important to consider all potential threat-sources that could cause harm to an IT system and its processing environment. For example, although the threat statement for an IT system, operative in a desert area, may not include natural flood, because of the low likelihood of occurrence of such an event, environmental threats such as a pipe burst can quickly flood a computer room and cause damage to an organization's IT assets and resources. Humans can become threat sources through intentional acts, such as deliberate attacks by malicious or disgruntled employees, or unintentional acts, such as negligence and errors. A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an IT system (e.g. via password guessing) in order to compromise system and data integrity, availability, or confidentiality or (2) a benign, but nonetheless deliberate attempt to circumvent system security. One example of the latter type of deliberate attack is a programmer writing a Trojan horse program to bypass system security in order to get the job done.

Motivation and Threat Actions

Motivation and the resources for carrying out an attack, make humans potentially dangerous threat sources. Table 3.1 presents an overview of many of today's common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack. This information will be useful to organizations, studying their human-threat environments and customizing their human-threat statements. In addition, reviews of the history of system break-ins, security violation reports, incident reports, and interviews with the system administrators, help desk personnel, and user community during information gathering, will help identify human threat

sources that have the potential to harm an IT system and its data and that may be of concern where vulnerabilities exist.

Table 3.1 Human-threats: threat source, motivation, and threat actions

<i>Threat Source</i>	<i>Motivation</i>	<i>Threat Actions</i>
Hacker, cracker	• Challenge • Ego • Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	• Destruction of information • Illegal information disclosure • Monetary gain • Unauthorized data alteration	• Computer crime (e.g. cyber stalking) • Fraudulent act (e.g. replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	• Blackmail • Destruction • Exploitation • Revenge	• Bomb/ Terrorism • Information warfare • System attack (e.g. distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	• Competitive advantage • Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	• Curiosity • Ego • Intelligence • Monetary gain • Revenge • Unintentional errors and omissions (e.g. data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data

(Contd)

<i>Threat Source</i>	<i>Motivation</i>	<i>Threat Actions</i>
		• Interception • Malicious code (e.g. virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack, should be made after the potential threat sources have been identified, in order to determine the likelihood of a threat, exploiting system vulnerabilities.

The threat statement or the list of potential threat sources, should be specific to the individual organization and its processing environment (e.g. end-user computing habits). In general, information on natural threats (e.g. floods, earthquakes, storms) should be readily available. Known threats have been identified by many government and private sector organizations. The use of intrusion detection tools is also becoming more prevalent, and government and industry organizations continually collect data on security events, thereby improving the ability to realistically assess threats.

Vulnerability Identification

The analysis of the threats to an IT system must include an analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by potential threat sources.

Table 3.2 Vulnerabilities and their threat sources

<i>Vulnerability</i>	<i>Threat Source</i>	<i>Threat Action</i>
Terminated employees, system identifiers (ID) are not removed from the system.	Terminated employees	Dialing into the company's network and accessing proprietary data.
Company firewall allows inbound telnet, and <i>guest</i> ID is enabled on XYZ server.	Unauthorized users (e.g. hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the <i>guest</i> ID.

(Contd)

<i>Vulnerability</i>	<i>Threat Source</i>	<i>Threat Action</i>
The vendor has identified flaws in the security design of the system. However, new patches have not been applied to the system as yet.	Unauthorized users (e.g. hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files, based on known system vulnerabilities.

VULNERABILITY

Vulnerability may be defined as a flaw or weakness in system security procedures, design, implementation, or internal controls that could get triggered accidentally or intentionally exploited and consequently, result in a security breach or violation of the system's security policy.

<i>Vulnerability</i>	<i>Threat Source</i>	<i>Threat Action</i>
Data center that is supposed to use water sprinklers to extinguish fire; tarpaulins to protect hardware and other equipment, from water damage, are not in place.	Fire, negligent persons.	Water sprinklers being turned on in the data center.

The recommended methods for identifying system vulnerabilities include, the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.

It should be noted that the types of vulnerabilities that exist, and the methodology needed to determine whether the vulnerabilities are present, will usually vary, depending on the nature of the IT system and the phase it is in, in the SDLC (System Development Life Cycle). If the IT system has not yet been designed, the search for vulnerabilities should focus on the organization's security policies, planned security procedures, and system requirement definitions, and the vendor's or developer's security product analyses (e.g. white papers). If the IT system is being implemented, identification of vulnerabilities should be expanded to include more specific information, such as the planned security features, described in the security design documentation and the results of system certification test and evaluation. If the IT system is operational, the

process of identifying vulnerabilities should include an analysis of the IT system security features and the security controls (technical and procedural), used to protect the system.

Vulnerability Sources

The technical and non-technical vulnerabilities, associated with an IT system's processing environment can be identified via the information-gathering techniques described earlier. A review of other industry sources (e.g. vendor web pages that identify system bugs and flaws) will be useful in preparing for interviews and in developing effective questionnaires to identify vulnerabilities that may be applicable to specific IT systems (e.g. a specific version of a specific operating system). The Internet is another source of information on known system vulnerabilities, posted by vendors, along with hot fixes, service packs, patches, and other remedial measures that can be applied to eliminate or mitigate vulnerabilities.

SYSTEM SECURITY TESTING

Proactive methods like employing system testing, can be used to identify system vulnerabilities. However, the efficiency of these methods will depend on the criticality of the IT system and available resources (e.g. allocated funds, available technology, persons with the expertise to conduct the test). Test methods include:

- Automated vulnerability scanning tool
- Security Test and Evaluation (ST and E)
- Penetration testing

The *automated vulnerability scanning tool* is used to scan a group of hosts or a network for known vulnerable services (e.g. system allows anonymous File Transfer Protocol [FTP], sendmail relaying). However, it should be noted that some of the *potential* vulnerabilities, identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment. For example, some of these scanning tools, rate potential vulnerabilities without considering the site's environment and requirements. Some of the vulnerabilities, identified by the automated scanning software, may not actually be vulnerabilities for a particular site, but may have been configured that way because their environment required it. Thus, this test method may produce false positives.

ST & E is another technique that can be used in identifying IT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g. test script, test procedures, and expected test results). The purpose of system security testing is to test the effectiveness of security controls of an IT system, that have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.

Penetration testing can be used to complement the review of security controls and ensure the security of the different facets of the IT system. Penetration testing, when employed in the risk assessment process, can be used to assess an IT system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the IT system, from the viewpoint of a threat source and to identify potential failures in the IT system's protection schemes.

DEVELOPMENT OF SECURITY REQUIREMENTS CHECKLIST

During this step, the risk assessment personnel determine whether or not the security requirements, stipulated for the IT system and collected during system characterization, are being met by existing or planned security controls. Typically, the system security requirements can be presented in a tabular form, with each requirement being accompanied by an explanation of how the system's design or implementation does or does not satisfy a particular security control requirement.

A security requirements checklist contains the basic security standards that can be used to systematically evaluate and identify the vulnerabilities of the assets (personnel, hardware, software, information), non-automated procedures, processes, and information transfers, associated with a given IT system, in the following security areas:

- Management
- Operation
- Technical

Table 3.3 lists the security criteria that can be used to identify an IT system's vulnerabilities in each security area.

Results of the checklist (or questionnaire) can be used as inputs for an evaluation of compliance and non-compliance. This process identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

Table 3.3 Security criteria

<i>Security area</i>	<i>Security criteria</i>
Management security	• Assignment of responsibilities • Continuity of support • Incident response capability • Periodic review of security controls • Personnel clearance and background investigations • Risk assessment • Security and technical training • Separation of duties • System authorization and re-authorization • System or application security plan
Operational Security	• Control of air-borne contaminants (smoke, dust, chemicals) • Controls to ensure the quality of the electrical power supply • Data media access and disposal • External data distribution and labeling • Facility protection (e.g. computer room, data center, office) • Humidity control • Temperature control • Workstations, laptops, and stand-alone personal computers
Technical security	• Communications (e.g. dial-in, system interconnection, routers) • Cryptography • Discretionary access control • Identification and authentication • Intrusion detection • Object re-use • System audit

Control Analysis

The goal of this step is to analyze the controls that have been implemented or are going to be implemented by the organization, to minimize or eliminate the likelihood (or probability) of a threat, exploiting a system vulnerability.

For example, a vulnerability (e.g. system or procedural weakness) is not likely to be exploited or the likelihood of its exploitation is low, if there is a

low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of harm.

Control Methods

Security controls encompass the use of technical and non-technical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g. access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Non-technical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical and environmental security.

Control Analysis Technique

As discussed earlier, the development of a security requirements checklist or use of an available checklist, will be helpful in analyzing controls in an efficient and systematic manner. The security requirements checklist can be used to validate security compliance as well as non-compliance. Therefore, it is essential to constantly update such checklists so that these can reflect the changes in an organization's control environment (e.g. changes in security policies, methods, and requirements) and also ensure the checklist's validity.

Determination of Likelihood

To arrive at an overall rating of likelihood, that indicates the probability that a potential vulnerability may be exploited within the construct of the associated threat environment, the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls

The likelihood that a potential vulnerability could be exploited by a given threat source, can be categorized as high, medium, or low. Table 3.4 below describes these three likelihood levels.

A threat is the potential for a particular threat source to successfully exploit a particular vulnerability. Vulnerability is a weakness that can get accidentally triggered or intentionally exploited. A threat source does not present a risk when there is no vulnerability that can be exploited. In determining the likelihood of a threat, one must consider threat sources, potential vulnerabilities, and existing controls.

Table 3.4 Definitions of likelihood levels and likelihood rating (high, medium, low)

<i>Likelihood level</i>	<i>Definition</i>
High	The threat source is highly motivated and sufficiently capable, and the controls to prevent the vulnerability from being exploited are ineffective.
Medium	The threat source is motivated and capable, but the controls are in place and may impede successful exploitation of the vulnerability.
Low	The threat source lacks motivation or capability, or the controls that are in place are capable of preventing, or at least significantly impeding, the vulnerability from being exploited.

Impact Analysis

The next major step in measuring the level of risk is to determine the adverse impact, resulting from the successful exploitation of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information, as has also been discussed earlier:

System mission (e.g. the processes, performed by the IT system)

- System and data criticality (e.g. the system's value or importance to an organization)
- System and data sensitivity

This information can be obtained from the existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A *mission impact analysis*, (also referred to as Business Impact Analysis [BIA] by some organizations) prioritizes the impact levels associated with the compromise of an organization's information assets, based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An *asset criticality assessment*, identifies and prioritizes the sensitive and critical information assets of an organization (e.g. hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

If this documentation does not exist or such assessments for the organization's IT assets have not been performed, the system and data sensitivity can be determined, based on the level of protection required to maintain the system's and data's availability, integrity, and confidentiality. Regardless of the

method used to determine how sensitive an IT system and its data are, it is the owners who are responsible for determining the impact level on their own IT system and information. Consequently, in analyzing, the impact, the most appropriate approach is to interview the system and information owner(s).

Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any of the following three security goals: *integrity*, *availability*, and *confidentiality*. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met with:

Loss of Integrity

System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance value of an IT system.

Loss of Availability

If a mission-critical IT system is unavailable to its end-users, the organization's mission may get affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus, impeding the end users' performance of their functions, in supporting the organization's mission.

Loss of Confidentiality

System and data confidentiality refer to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from jeopardizing national security to disclosing the privacy Act of individuals which has legal implications. Unauthorized, unanticipated, or unintentional disclosure could result in a loss of public confidence, embarrassment, or initiation of legal action against the organization.

Some tangible impacts can be measured, quantitatively, in terms of the revenue lost, cost of repairing the system, or the level of effort required to correct the problems, caused by a successful threat action. Other effects, like the loss of public confidence, loss of credibility, damage to the organization's interest, etc., cannot be measured in specific units, but can be qualified or

described in terms of high, medium, and low impact. Because of the generic nature of this discussion, this guide describes only the qualitative categories—high, medium, and low impact (see Table 3.5).

Table 3.5 Definitions of magnitude of impact

<i>Magnitude of impact</i>	<i>Definition</i>
High	Exploitation of the vulnerability may (1) result in a significant, monetary loss of major tangible assets or resources; (2) significantly violate, harm, or impede an organization's mission, reputation, or interest or (3) may result in human death or serious injury.
Medium	Exploitation of the vulnerability may (1) result in loss of tangible assets or resources; (2) violate, harm, or impede an organization's mission, reputation, or interest; or (3) result in human injury.
Low	Exploitation of the vulnerability may (1) result in the loss of some tangible assets or resources or (2) noticeably affect an organization's mission, reputation, or interests.

Quantitative versus Qualitative Assessment

In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments. The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement, in addressing the vulnerabilities. The disadvantage of the qualitative analysis is that it does not provide specific, quantifiable measurements of the magnitude of the impact, therefore, making a cost-benefit analysis of any recommended control, difficult.

The major advantage of a quantitative impact analysis is that it provides a measurement of the magnitude of the impact which can be used in the cost-benefit analysis of recommended controls. The disadvantage is that, depending exclusively on the numerical ranges, used to express the measurement, may make the meaning of the quantitative impact analysis unclear and may require the result to be interpreted in a qualitative manner. Often additional factors must also be considered to determine the magnitude of impact. These factors may include, but are not limited to:

- An estimation of the frequency of exploitation of the vulnerability by the threat source over a specified time period e.g. one year

- An approximate cost analysis of each occurrence of the threat source's exploitation of the vulnerability
- A weighted factor, based on a subjective analysis of the relative impact of a specific threat, exploiting a specific vulnerability

Risk Determination

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of:

- The likelihood of a given threat source's attempt to exploit a given vulnerability
- The magnitude of the impact, should a threat-source successfully exploit the vulnerability
- The adequacy of planned or existing security controls for reducing or eliminating risk

To measure risk, a risk scale and a risk-level matrix must be developed.

Risk-Level Matrix

The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g. probability) and threat impact. Table 3.6 below shows how the overall risk ratings may be determined, based on inputs from the threat likelihood and threat impact categories. The matrix below, is a 3 × 3 matrix of threat likelihood (high, medium, and low) and threat impact (high, medium, and low). Depending on the site's requirements and the granularity of risk assessment desired, some sites may use a 4 × 4 or a 5 × 5 matrix. The latter can include a very low/very high threat likelihood and a very low/very high threat impact to generate a very low/very high risk level. A very high risk level may require a possible system shutdown or stopping of all IT system integration and testing efforts.

The sample matrix in Table 3.6 shows how the overall risk levels of high, medium, and low are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For example, the probability assigned for each threat likelihood level is 1.0 for high, 0.5 for medium, and 0.1 for low. The value assigned for each impact level is 100 for high, 50 for medium, and 10 for low.

Table 3.6 Risk-level matrix

Threat likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low $10 \times 1.0 = 10$	Medium $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Medium (0.5)	Low $10 \times 0.5 = 5$	Medium $50 \times 0.5 = 25$	Medium $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)8.

Description of Risk Level

Table 3.7 describes risk levels shown in the above matrix. This risk scale, with its ratings of high, medium, and low, represents the degree or level of risk to which an IT system, facility, or procedure may be exposed if a given vulnerability were exploited. The risk scale also presents actions that the senior management, the mission owners, must take for each risk level.

Table 3.7 Risk scale and necessary actions

Risk level	Risk description and necessary actions
High	If an observation or finding is evaluated as a high-level risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as a medium-level risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as a low-level risk, the system's owner must either determine whether corrective actions are still required or decide to accept the risk.

If the level indicated against certain items is so low as to be deemed “negligible” or insignificant (value is <1 on a risk scale of 1 to 100), one may wish to keep these aside and forward them to the management for the requisite action. This will ensure that these are not overlooked, when conducting the

next periodic risk assessment. It also helps establish a complete record of all the risks identified during the analysis exercise. These risks may move to a new risk level, on reassessment, due to a change in threat likelihood and/or impact and that is why it is critical that they not be ignored during the exercise.

Control Recommendations

During this step of the process, controls that could mitigate or eliminate the identified risks and that are appropriate to the organization's operations, are provided. The goal of recommending controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options, e.g. system compatibility
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability

The control recommendations are results of the risk assessment process and provide input to the risk mitigation process, during which the recommended, procedural and technical security controls are evaluated, prioritized, and implemented.

It should be noted that not all recommended controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis should be conducted for the proposed, recommended controls, to see if the costs of implementing the controls can be justified by reduction in the level of risk. In addition, the operational impact, e.g. effect on system performance, and feasibility, e.g. technical requirements, user acceptance, etc. of introducing the recommended option should be evaluated carefully during the risk mitigation process.

Documentation

Once the risk assessment has been completed, i.e. threat-sources and vulnerabilities have been identified, risks assessed, and recommended controls provided, results should be documented in an official report or briefing.

A risk assessment report is a management report that helps the senior management, and mission owners, to make decisions on policy, procedural, budget, and system operational and management changes.

Some organizations prefer to start the risk management process with the identification of threats, rather than assets. It is important for the IS auditors to understand that there is a wide variety of formal and informal approaches available for risk assessment and management. The IS auditor should not be concerned about which approach is adopted, and whether one approach is intrinsically better than the other, but should be able to critically appraise the thought process that the management has employed to identify and evaluate risks and come to a decision about which risks to minimize.

Although the risk analysis model of assessing control described above has now gained prominence in the industry, another common model for assessing control is the process audit model. This model approaches the control at the process (COBIT) level and has a four prong approach, i.e.:

- *Obtaining* an understanding of business requirements, related risks, and relevant control measures
- *Evaluating* the appropriateness of stated controls
- *Assessing* compliance, by testing whether or not the stated controls are working as prescribed, consistently and continuously
- *Substantiating* the risk that the control objectives are not being met, by using analytical techniques and/ or consulting alternative sources.

COBIT has developed this structure into an audit framework, by providing audit guidelines which are available at www.isaca.org for the members of ISACA.

A typical audit cycle, advocated by many professional audit bodies, including the American Institute of Certified Public Accountants is depicted below. While both external and internal auditors can follow the generic approach depicted in the flowchart (Fig. 3.1) here, the decisions they take at each step may vary because of their role difference. For example, an internal auditor may spend more time testing controls because they are more concerned about the efficiency of controls than external auditors.

CONDUCTING IS AUDIT FOR BANKS

Conducting Information System Audit for banks is no different from conducting it for any other organization. The only important point for IS Audit of banks is to know the regulatory framework within which the banks are functioning and the existing guidelines and standards applicable to the sector.

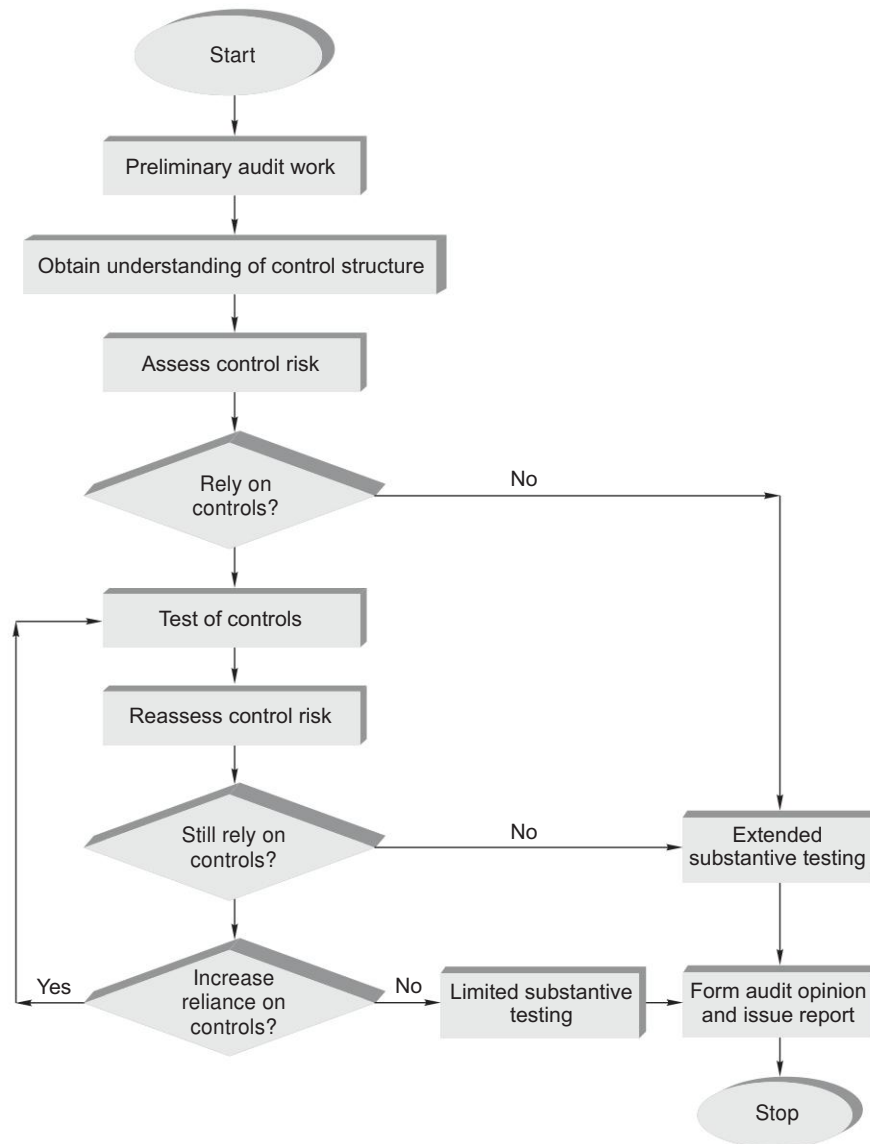


Fig. 3.1 Generic flow chart of an audit

Therefore, instead of going into the various steps of IS Audit in banks, it will be more useful to discuss some of the regulatory guidelines issued by the Reserve Bank of India and their implications.

Reserve Bank of India constituted a 'Working Group for Information Systems Security for the Banking and Financial Sector', under the chairmanship of Dr R.B. Barman, Executive Director, RBI, to finalize the standards

and procedures for IS audit and IS security guidelines for the banking and financial sector.

This report discusses various aspects of IS audit such as its objectives, approaches, methodology, charter, planning, standards and guidelines, sampling, evidence, and documentation. It also discusses the skills that IS auditors are required to possess and the way they will be required to address the irregularities observed.

The IS audit policy issues and the IS security guidelines, discussed in this report, are only indicative and each bank has to devise its own security controls, on an on-going basis and enhance the same, as required, from time to time.

A summary of the recommendations and their brief explanation is given below.

1. Each organization in the banking and financial sector in the country should formulate its security policy on the lines of the guidelines, as set out in the 'Information Systems Security Guidelines' (Annexure to the Information System Audit document).
2. Well-planned and structured audit is essential for risk management, and monitoring and control of Information Systems in any organization. Therefore, each bank should have a structured work area, viz. Information System Audit, with clearly defined lines of responsibilities and autonomy.
3. Banks and financial institutions should use the services of the Certified Information Systems Auditors (CISA), Certified Information System Security Professionals (CISSP), etc. for the conduct of IS Audit in their respective organizations.
4. Audit findings and conclusions should be supported by appropriate analysis and interpretation of the evidence/information gathered.
5. As far as possible, evidence should be independent in nature.
6. The IS auditor should consider whether the policies issued, cover all the appropriate areas for which board-level direction is necessary, in order to provide reasonable assurance that the business objectives have been achieved. Policies, on board-level direction, should be documented ones only and such documented policies should, among others, include the following:
 - (a) Security policy
 - (b) Human resources policy
 - (c) Data ownership policy
 - (d) End-user computing policy

- (e) Copyright policy
 - (f) Data retention policy
 - (g) System acquisition and implementation policy
 - (h) Outsourcing policy
 - (i) The IS auditor should consider the position or functions of IS specialist staff in the organization and assess whether these will enable the organization make the best use of IS to achieve its business objectives.
7. The control of the Information Systems, even in decentralized and end-user run environments, should include a segregation of conflicting or overlapping duties.
 8. The IS audit should cover all the computerized departments/ offices of the organization.
 9. IS auditors should employ the manual procedures, when they are more effective than other alternatives or when the procedures cannot be partially or fully automated. He/she should also use computer assisted procedures and Computer Assisted Audit Techniques (CAATs) because they permit the IS auditors to switch from the procedures based on limited, random, and statistical samples of records in a file, to procedures that include every record in a file.
 10. There should be an audit charter or engagement letter that appropriately documents and defines the responsibility, authority, and accountability of the IS audit function, both internal and external. The IS auditor should determine how to achieve the implementation of the applicable IS audit standards, use professional judgment in their application, and be prepared to justify any departure therefrom.
 11. The IS auditor should have a clear mandate from the organization to perform the IS audit function. This mandate is ordinarily documented in an audit charter, which should be formally accepted by the IS auditor. The audit charter, for the audit function as a whole, should include the IS audit mandate.
 12. IS auditing should be performed by personnel who possess the required expertise and skills, such as the Certified Information Systems Auditor (CISA), Certified Information Systems Security Professionals (CISSP), etc.
 13. The major areas, which should be IS audited, are broadly as under:
 - (a) Safeguarding of assets
 - (b) Data integrity

- (c) System effectiveness
 - (d) System efficiency
 - (e) Organization and administration
 - (f) Business continuity operations.
14. The IS auditor should have the following skills to be able to perform his/her duties effectively:
- (a) A general understanding of the operating systems in use
 - (b) Thorough knowledge of application software in use
 - (c) Knowledge of the automated operations, methods of storing and retrieval of data, and controls used in the systems
 - (d) Knowledge of the methodology used in data processing
 - (e) Substantial knowledge about development, implementation, and operation of the systems. A thorough understanding of various controls in the development of systems, maintenance of data, and network management is also essential
 - (f) An understanding of the emerging technologies, capacity to determine their impact on controls, ability to change audit procedures suitably, and to develop evidence/information collection tools and techniques
 - (g) The IS auditors, to be engaged, should maintain technical proficiency and keep themselves abreast of the current changes in the procedures, technologies adopted, and the functions computerized by organizations in the banking and financial sector
 - (h) Ability to identify general security measures, including risk analysis
 - (i) Capability for undertaking constructive disaster assessment
 - (j) Sound knowledge of the organization's accounting practice and record-keeping requirements
 - (k) Ability to investigate thoroughly and to document the investigation work
 - (l) Initiative, thoroughness, and tact while conducting an audit assignment
 - (m) The understanding and the ability to analyze and offer constructive comments on the IS security and controls
 - (n) All material irregularities are required to be reported and the IS auditor should report even the unpleasant findings

- (o) Awareness of situations, where too much trust has been placed in one individual. One person, acting alone could commit an error willfully or defraud the organization. This is important especially in those transactions, which are perceived to be of a high risk level
 - (p) Capacity to plan and supervise IS audit to ensure that the audit achieves the desired objectives, as set out in the audit assignment, efficiently
 - (q) Knowledge of the basics in computer programming for clarity of approach.
15. The IS auditor should prepare and retain documentation to support the audit work performed. The IS auditor should apply internationally accepted IS auditing standards to the performance of the IS audit, use professional judgment in the application of such standards, and be prepared to justify deviation, if any, therefrom.

Besides this, the RBI has also come out with generic checklists of IS audit in the following areas:

1. Business strategy
2. Long-term IT strategy
3. Short-range IT plans
4. IS security policy
5. Implementation of security policy
6. IS audit guidelines
7. Acquisition and implementation of packaged software
8. Development of in-house and outsourced software
9. Physical access controls
10. Operating system controls
11. Application systems controls
12. Database controls
13. Network management
14. Maintenance
15. Internet banking

These checklists also can be accessed from the website of the RBI at <http://www.rbi.org.in>. These IS audit checklists prepared by the RBI, are platform-independent, and necessary platform-dependent audit checklists can be framed by the banks themselves. On the basis of the practices followed by individual banks, they may frame bank-specific audit checklists.

THE ROAD MAP FOR SETTING UP INFORMATION SYSTEM AUDIT FRAMEWORK FOR THE BANK

Now that the computerization in the banking industry has gained width and depth, it is imperative for the bank's management to set up a framework for information security and audit which will help in ensuring that the business objectives are realized.

A discussion on framework would be incomplete without knowing what exactly a framework is. A framework is the basic support structure, designed to support or enclose something. An IS audit framework is the structure within the organization, which is designed to support the IS audit function.

When organizations design their own framework, depending on their business requirements, priorities, existing infrastructure, etc. the following points should be kept in mind:

- The organizational structure
- The existing infrastructure and the future plan
- The required skill sets
- Monitoring

A proposed framework, suggested by the authors, is furnished below, which can be used as a reference by banks.

Pillars of the Information System Audit/ Security Framework

Framing Security Policy

The first stage in constructing information security framework is “framing the information security policy”. Now certain questions arise, viz. Who should draft the policy? What should it contain? Are there any standards for an information security policy? How is it to be implemented? And finally how is it to be updated? To answer all these questions in detail is not in the scope of this chapter, but in a nutshell, a security policy should be drafted by a group of people who are conversant both, with the control philosophy and the banking domain. Whether in-house or outsourced is not the main issue. The security policy is a vital and high-level document and it should contain control guidelines for Information Systems, starting from acquiring the system to its disposal. The operational procedures are not part of the security policy. In fact, there is a one-to-many relationship between policy and procedures, i.e. for a

single high-level policy there can be many operational procedures and it is for the bank to choose the appropriate procedures, depending on the technology and the risks involved. At present, the British Standard 7799 and ISO17799 are gaining prominence as the standards for information security. The control objective for information and related technologies (COBIT), a product of IT Governance Institute, USA, also provides standards for high-level control objectives. The implementation of a security policy requires the support of the top-level management and also cooperation, down the line. The updation policy of the security policy is a part of the main document.

If a group of 4–5 officials in a large bank are involved in framing a draft enterprise security policy, its completion should not take more than two months. During these two months, the group should gather the existing documents, viz. existing computer operation manual, user manual of the existing application, the government and regulator's guidelines, if any, and users' feedback. The group can also prepare some customized questionnaires and circulate them among a large number of users/administrators, etc. Such a study is required to analyze the existing risks and controls so that the control gaps can be bridged through recommendations in the policy.

Management's Approval

The next stage in the framework is presenting the policy to the top-level management for its approval. The scope, objective, implementability, and essence of the policy should be clearly mentioned in the presentation. Although the economic aspect of policy implementation, i.e. approximate amount required to be spent, should also be explained there cannot be any objective Return on Investment (ROI) drawn for the implementation of the security policy. The tentative date of the implementation of the policy should also be a part of the presentation. This date should not be less than two months from the date of approval because there is another stage called the awareness stage in between.

The presentation and policy approval stage should not take more than a month.

Awareness Program

Once the policy is approved, the next step is creating awareness about the policy among the employees/people who are covered by it. The copy of the approved policy should be made available to all the permanent employees of the organization, whereas for others, including third party contractors, relevant portions can be made available. The awareness program can be in the form of

seminars, workshops, notices on bulletin boards, E-Mail, posters, etc. The corporate intranet of the organization can be used as a vehicle for this awareness program, which can also be employed for evaluation of the success of the awareness program, through customized questionnaires. The “know your bank” scheme, launched by some banks may be improvised to receive inputs about the success of the awareness program and appropriate award/ incentives can also be instituted for this exercise.

The awareness program, to be successful should be conducted across the organization in different places simultaneously. The entire process should not take more than two months.

Implementation Strategy

Once the awareness program is complete, it's time to implement the policy. The old concept of a 'phased' implementation, i.e. implementation of the policy in some branches at a time per month or so, is unlikely to work because today, the geographical boundary of the organization has been reduced due to networking and breaches can be committed by any branch. So there has to be a big-bang approach in the implementation, i.e. enterprise-wide implementation.

Continuous Monitoring

Once the security policy is implemented there should be a mechanism for continuous monitoring of the policy to ensure whether it has been implemented in its true spirit or not. Also, since security itself is very dynamic, there should also be a structured mechanism to update the policy, as and when required. The framework itself should be made intelligent enough to trigger the management about the need to update in the policy. The assurance mechanism, in the form of audit, should also be a part of the framework.

Risk Profiling of the Branches

Once the first phase of the training plan is over, the organization should get ready for the assurance exercise, i.e. audit of the selected branches. Although, for selecting branches for the first phase of audit, we need to do a thorough risk profiling of the branches, at this stage it is always recommended to perform a risk profiling exercise, taking objective parameters into consideration. The parameters could be asset value, turnover, level of computerization, etc. It would be advisable to include all the fully-computerized branches and also those that have opted for centralized solutions.

Empanelment of External Auditors

Now it is time to empanel qualified/experienced auditors to audit the branches, as per the risk profiling done earlier. The request for a proposal for empanelment should *inter alia* include the number of CISA qualified auditors in the firm, experience in the banking and financial sector in similar audit exercises, all-India presence, financial standings, etc. The scope of work should emphasise application control review and security audit. At this stage, the bank should not give the auditors a checklist for conducting the audit. The auditors should be allowed to do their work independently, without depending on the checklist.

Evaluation of Reports

Once the auditors submit their reports, these need to be analyzed by the management and also by 'focused' groups. The work of such a group would be, taking the inputs from various reports and using these as the base documents for preparing an audit manual for the bank. These audit guidelines can be used by various delivery channels of the bank, i.e. internet banking, ATM, etc. As the audit reports prepared by the auditors are the first such reports after the implementation of security policy, the inputs from these can be taken for updation of the policy and also further retraining of officials.

After this phase, it is presumed that the officials posted in the focused areas have got some exposures on risks and controls in banks. Therefore, it's time to plan for a gradual reduction in dependence on outsourced audit and develop a strong in-house expertise. The next phase of audit should involve, both external and internal auditors. The audit work of the branches, which was being done by external auditors, should now be given to the internal auditors and the work of the new branches, should be allotted to external auditors. This is also the time when the bank should prepare the audit charter.

The next stage is again analyzing the reports submitted both, by in-house and outsourced auditors. Inputs from these reports should also be taken for updating the security policy, audit manual, and for further training, as and when required.

Such iterations should go on till the bank develops a dedicated IS audit team and manages to reduce its dependence on external auditors.

Proposed Framework

The proposed framework, depicted in Fig. 3.2, the diagram takes into account the stages involved in framing and implementing the security policy discussed above, and also uses the IS audit for making the system more reliable and effective.

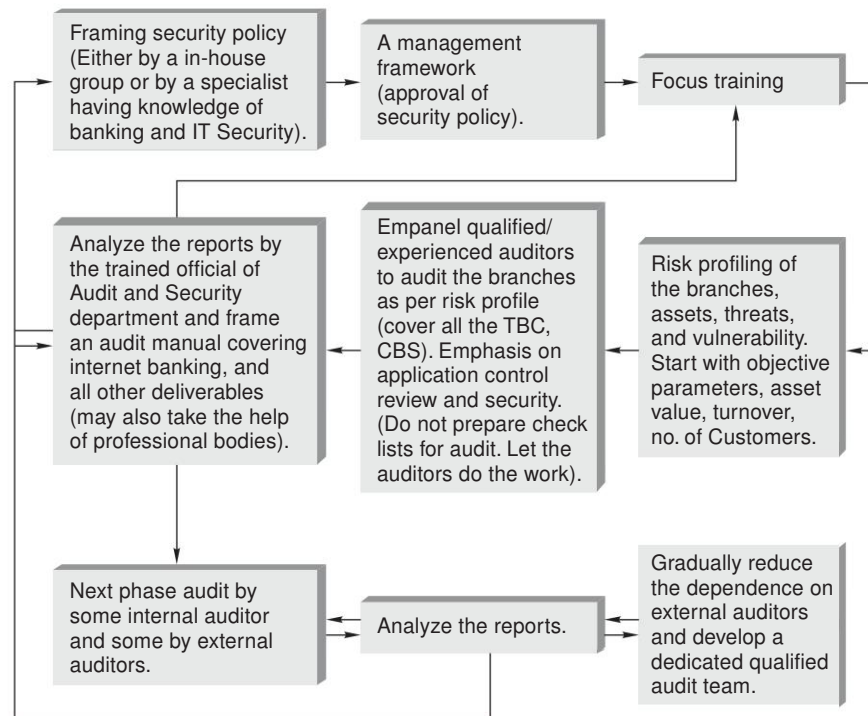


Fig. 3.2 Proposed information assurance framework

SUMMARY

In this chapter, we first learnt about the audit charter and engagement letter. What are these? What should these contain? We also saw a model audit charter for a bank. Then we discussed audit planning, its elements, audit methodologies, resources planning, etc. Risk assessment which is a part of audit planning, was also discussed at length, together with the methodologies adopted by International Standard Organization (ISO). These include asset cataloguing (which we call system characterization), threat, vulnerability analysis, likelihood analysis, drawing up of a risk-level matrix, etc. Then we discussed the various stages of conducting audit and depicted these in generic flow chart. The various guidelines issued by the Reserve Bank of India about Information System Audit were also discussed briefly. And finally, we discussed a generic Information System Audit framework which can be set up by a bank to help in the protection of its information assets.

REVIEW QUESTIONS

1. What is an audit charter and an audit engagement letter? How are they different? What should these contain? Write a model engagement letter.
2. What is audit planning? Why is it required? List the elements of audit planning.
3. What is risk assessment? Write about the five variables, used for risk assessment.
4. What are the risk assessment methodologies proposed by the National Institute of Standard & Technology (NIST)? Write in detail, about each step.
5. What is impact analysis from the risk assessment point of view? Discuss in detail with the help of a risk-level matrix.
6. What are the various steps involved in conducting Information System Audit? Discuss with the help of a flow chart.
7. What are the various guidelines issued by the Reserve Bank of India about conducting Information System Audit for banks in India? Discuss.
8. What is a framework? Describe the Information System Audit framework discussed in the chapter.

MULTIPLE CHOICE QUESTIONS

1. Audit charter is a document:
 - (a) Prepared by the organization for the operation of the Internal Audit department
 - (b) Prepared by the auditee for the auditors
 - (c) Prepared by the organization for the internal control and audit function, which states the auditor's responsibility, function, and scope of authority
 - (d) Prepared by the organization for the internal control and audit function, which states the management's responsibility, scope of authority, and accountability to the IS audit function
2. Engagement letter in Information System Audit refers to:
 - (a) Letter from the auditee to the auditor
 - (b) Letter from the auditor to the auditee, mentioning the auditor's role, responsibility, scope of authority, and accountability
 - (c) A part of the audit charter, meant for the external auditor

112 *Information System Audit and Assurance*

- (d) A letter from the management to the external auditor, describing the role and responsibility of the auditor for that particular assignment
- 3. In an audit engagement letter, “agreed completion date” falls under the category of:
 - (a) Accountability
 - (b) Authority
 - (c) Responsibility
 - (d) Authority and responsibility
- 4. For understanding the auditee’s organization, the auditor should:
 - (a) Visit the website of the auditee
 - (b) Interact with the competitors
 - (c) Interview the IT department personnel
 - (d) Review previous reports
- 5. Risk assessment is conducted:
 - (a) Before the planning stage of the audit
 - (b) At the planning stage
 - (c) At testing of the control stage
 - (d) It is not a part of the audit function
- 6. Vulnerability of an asset:
 - (a) Is a weakness that can be accidentally triggered
 - (b) Is a weakness which can be intentionally triggered
 - (c) Is a weakness which can be triggered both accidentally or intentionally
 - (d) Is a weakness of the asset
- 7. If the IT system has not yet been designed, the search for vulnerabilities should focus on:
 - (a) Planning and organization
 - (b) Organizational security policy and procedures
 - (c) System requirement definitions, if any
 - (d) B and C
- 8. The purpose of the system security testing is to:
 - (a) Test the effectiveness of the security control
 - (b) Test the efficiency of the security control
 - (c) Test the data integrity
 - (d) Test the effectiveness of the security control when applied to an operational environment

9. The four-prong approach of audit, devised by COBIT is:
 - (a) Obtaining, evaluating, assessing, and substantiating
 - (b) Evaluating, assessing, monitoring, and substantiating
 - (c) Assessing, evaluating, substantiating, and reporting
 - (d) Evaluating, assessing, monitoring, and substantiating
10. If the auditors do not rely on the internal controls of the organization, then:
 - (a) More substantive tests should be conducted
 - (b) More compliance tests should be conducted
 - (c) Control risk should be reassessed
 - (d) Management should be informed

DISCUSSIONS AND RESEARCH QUESTIONS

1. 'Information System Audit is nothing but evaluation of internal control.' Critically discuss the statement.
2. To differentiate between **possible** and **probable** threats, which can exploit the vulnerabilities of the assets and cause losses, is very important from an IS auditor's perspective. Critically analyze the statement.
3. Discuss how a perfect audit plan helps in the organizational resources planning.
4. Establishing an intelligent IS security and audit framework is necessary for the organization for protecting the organization's information assets. Discuss.
5. Describe the pillars of Information System security and audit framework, discussed in the chapter.

EXERCISES

1. Develop a security requirement checklist for a bank.
2. Develop customized questionnaires, which need to be administered to the top-level management of a bank, for determining security awareness in the organization.
3. Write down the steps for conducting a review on determining the efficiency of a software application.
4. What are the prerequisites for conducting an impact analysis? Devise a framework for conducting impact analysis of a bank in a fully-computerized environment.

4

Management Control Review

-
-
- ❖ Defining a strategic IT plan
 - ❖ Long and short-range plan
 - ❖ IS management architecture
 - ❖ Evaluating the organizing function
 - ❖ Policy and procedures
 - ❖ Human resources policy
 - ❖ Outsourcing practices
 - ❖ Organization of IS function
 - ❖ Separation of duties control matrix
 - ❖ Evaluation of leading function
 - ❖ Evaluation of controlling function
 - ❖ Auditing the management control
 - ❖ Checklist for auditing management control framework of IS
-
-

Often, Information Technology has been viewed and dealt with as a purely technological matter and very little effort has been made to link it with and treat it as one of the vital priorities and requirements. Consequently, the responsibility of governing and managing activities related to IT, has been entrusted to the operational and technical managers. But technology is more of a management concern than a purely technological one. As such, the management's commitment to IT is essential, to make the information resource-owners and users aware of this crucial issue and to provide the visibility, needed by the IS technology team to ensure support from business units.

While the traditional objective of IT in an organization has been, “protecting the interests of those relying on information, and on the systems and communications that deliver the information, from harm resulting from failures of *authenticity*, *confidentiality*, and *integrity*”, emerging definitions are adding concepts like availability, utility, and ability to cope with theft, deception, and fraud, etc. IT. Thus, information security seeks to meet the ambit of owner’s need to preserve the availability, utility, integrity, authenticity, confidentiality of information protect it from accidental and intentional acts of abuse and misuse. It seeks to control the forces that could cause destruction or copying, interference with use, use of false data, modification or replacement, misrepresentation or repudiation, misuse or failure to use, finding or taking, disclosure or observation, etc. For this, a suitable strategy should ensure, avoidance and deterrence, prevention and detection, mitigation and investigation, sanctions and rewards, recovery and correction, and finally education. Accordingly, the enterprise-specific safeguards and practices are to be selected with due care.

The objectives set above require a mix of technology and management control, with the management control having a definite priority over the former. There cannot be any exclusive technological solution to a management problem. However, there can be a managerial solution to a technological problem.

In this chapter, we will outline the management controls required for Information Systems, how these need to be exercised and what assurance mechanisms are needed to give a reasonable assurance to the management that the Information Systems are safeguarding assets, maintaining data integrity, fulfilling the organizational goals effectively, and consuming resources efficiently.

MANAGEMENT CONTROL

From an organizational point of view, the management is answerable to the stakeholders and hence, is responsible for all the organizational activities. But we will restrict our discussion to the role of the management and its responsibilities in managing Information Systems. In this context, the management level roles can be broadly classified into four categories (Weber Ron), viz. *planning*– which involves determining the goals of the Information Systems which should be aligned with the business goals and which should facilitate their achievement; *organizing*– i.e. gathering, allocating, and coordinating the resources needed to accomplish the goals; *leading*– i.e. motivating, guiding and communicating with the personnel and *controlling*– i.e. comparing actual performance with planned performance, as a basis for taking any corrective actions that are needed.

For performing all the above activities successfully, the management needs an independent entity to give them the assurance that they are on the right path. Here, the role of the auditor becomes vital. In the following sections, we will discuss the major management functions (standard practices) that fall under the above given heads (planning, organizing, leading, and controlling) and how they should be performed in the context of the Information System. Then we will discuss the role of the auditors in assuring the management that the Information System fulfills the organizational objectives.

PLANNING

Defining a Strategic Information Technology Plan

The senior management is responsible for developing and implementing long and short-range plans that fulfill the organization's mission and goals. In this respect, the senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the organization's long and short-range plans. These plans should be developed in a way that will ensure that the use of IT is aligned with the mission and business strategies of the organization.

IT Long-Range Plan

IT management and business process owners are responsible for regularly developing IT long-range plans (i.e. plans developed for over one year and less than five years) that will support the achievement of the organization's overall mission and goals. The planning approach should include mechanisms that solicit input from relevant, internal and external stakeholders, affected by the IT strategic plans. Accordingly, the management should implement a long-range planning process, adopt a structured approach, and set up a standard plan structure.

What a Long-Range IT Plan should Contain

Long-range IT plan should cover the basic questions of what, who, how, when, and why i.e. what needs to be done? Who should be involved in the process? How can the objective be achieved? When should the process start and by when should it be completed? And above all, why should these things be done? The IT planning process should take into account risk assessment results, including business, environmental, technology, and human resources risks.

Aspects which need to be adequately addressed during the planning process, include the organizational model and changes made to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third parties or the market, planning horizon, business process re-engineering, staffing, in or outsourcing, data, application systems, and technology architecture. Benefits of the choices made should also be clearly identified. It is a good idea to include performance indicators and targets in the plan.

How Often the Plan Should be Changed/Modified

There should be a proper change management procedure for change and modification of the long-range IT plan. These modifications should be carried out in a timely and accurate manner, to accommodate changes in the organizational strategy.

Short-Range Planning for the IT Function

Short-range plans are basically operational plans, which are translated at regular intervals from long-range IT plan. Such short-range plans should ensure that appropriate IT function resources are allocated, on a basis, consistent with the long-range IT plan. The short-range plans should be assessed periodically and amended, as and when necessary, in response to changing business and IT conditions. The timely performance of feasibility studies can ensure that the execution of the short-range plans had been initiated appropriately.

Communication of IT Plans to Relevant Parties

The management should ensure that long and short-range IT plans are communicated to business process owners and other relevant parties across the organization. In fact, the relevant portions of the plan should be made known to the respective process owners.

Monitoring and Evaluating IT Plans

The management should establish processes to capture and report feedback from business process owners and users, regarding the quality and usefulness of long and short-range plans. Feedback obtained should be evaluated and considered for future IT planning.

Assessment of Existing Systems

Prior to developing or changing the strategic or long-range IT plan, the IT management should assess the existing Information Systems, in terms of the degree of business automation, functionality, stability, complexity, costs, strengths, and weaknesses, in order to determine the degree to which the existing systems support the organization's business requirements.

The amount of resources the organization spares for planning is again directly proportional to the dependence of the organization on Information System. For example, in case of a bank, opting for core banking and other, related delivery channels, the planning process should be rigorous and the organization should spend comparatively more resources for planning.

Now, once the goals are laid down in the plan, the organization should devise various means to achieve these goals and one of the important means of achieving the goals is to put in place an Information System management architecture.

INFORMATION SYSTEM MANAGEMENT ARCHITECTURE

Since the ultimate responsibility of the performance of the organization rests with the top-level management, there should be a definite framework established by the management, which should include the management architecture, i.e. forming IT steering committees, focused groups, etc., clear specification of roles and responsibilities, etc. While setting up a framework, the following fundamental concepts should be borne in mind:

- The framework should be based on the idea of teamwork rather than a hierarchical setup
- There should be a proper segregation of duties and the personnel should not be assigned overlapping or conflicting responsibilities
- There should not be too many committees, as the focus, in such a situation, may be lost
- There should be decentralization of financial/administrative decision-making for effective IT implementation
- The steering committee should be a mix of IT and functional experts
- Top-level management should be involved for providing strategic inputs and not for operational matters

- Help of reputed institutions, with expertise in both domain knowledge and technology must be taken especially for giving the initial direction to the setting up a framework

SETTING UP OF AN INFORMATION TECHNOLOGY FRAMEWORK FOR A BANKING ORGANIZATION

Information Technology in the banking and financial sector in India, is no more an option for the management of these institutions. Banks have to go in for multiple IT-enabled delivery channels, otherwise they are likely to lose their customers and may also be unable to reap the benefits of the competitive advantages of Information Technology. In fact, Information Technology has crossed the line, from being just an enabling tool to being integrated/ interwoven with business processes. Once it becomes a part and parcel of the business process, calculating the Return on Investment on IT per se, will not be of much use because there are lots of intangible benefits that result from successful IT implementation. Let us take the example of online ATM implementation. IT expenditure on elements like the ATM switch, software licenses, training, and other network components will be definitely high. But we should not ignore the fact that the deployment of these components also opens up an additional delivery channel for the banking operations. As a result, there is every likelihood of a significant migration of retail transactions from the branch to the ATM channel. Once that happens, the transaction cost in ATMs will also be reduced significantly, to even upto 60%, if the number of ATMs reaches the critical mass level. This percentage value should then be treated as a payback to the IT department and shown as cost recovery or profit earned by it. Here, although a direct ROI is not worked out, the assessment of the values of the investments can be made by recognizing the following:

- (a) An increase in revenue from operations
- (b) A steady business growth possible due to branch expansion in a compressed timeframe
- (c) Acquisition of new customers
- (d) Fewer requirements for skilled IT manpower, to manage operations at each branch

Investment in Information Technology is not a one-time effort. In fact, we are of the view that for reaping the maximum benefit from Information Technology, the bank should not only opt for core banking, internet banking, and other IT-enabled delivery channels, but also integrate all other enterprise applications like HR/Pay Roll/and all other work flow processes. For this,

investment in IT infrastructure has to be given greater importance and it should be borne in mind that such investment has to be undertaken on an on-going basis and may be gradually increased each time, till the IT infrastructure becomes resilient and self-sufficing.

Box 4.1

Disruptive technology

Bower and Christensen, in their work on disruptive technologies, describe how most managers are trained to listen to their customers' needs when developing new products or adding new features to existing technologies. This approach of "the customer is always right", may not be appropriate under all conditions. For example, in a situation where a new technology is being evaluated and the customers don't appear to be excited about the benefits of the technology, a decision by the management to allocate resources to acquire such technology will be a difficult one, notwithstanding the fact that the new technology has got first mover advantages for the organization. Technology that is disruptive, typically offers customers a basket of attributes that are different from what the customers valued earlier. When launched initially, they perform below the customers' expectations on a few dimensions, but the performance trajectory of disruptive technologies tends to be very stiff. The new technology starts to outperform the older established technology and creates a whole new market and product paradigm. A case in point is the transistor radio launched by Sony in the 1950s. At that time, radios were made of vacuum tubes and were large and bulky. High fidelity of sound was the important attribute, valued by the listeners. Sony's transistor, initially compromised on sound fidelity, but provided a new attribute, that is portability. Over a period of time, this attribute forced a paradigm shift in the way the people listened to the radio and gradually the portable radio replaced the radio with vacuum tubes. Before launching this product, had Sony asked for feedback from its existing customers, it would have probably got responses that would have discouraged Sony from launching the new product.

There may arise certain questions in the mind of the management, like How do we get Information Technology under control, so that it delivers the information the organization needs? How do we manage risks and secure the infrastructure we are so dependent on? The answer to all of the above is establishing an Information Technology framework with policies, procedures, clear lines of responsibility, and above all top-level management support.

The framework should have the board of directors at the top followed by board-level sub-committees and down the line there should be executive steering committees and then focused work areas. The roles and responsibilities of the various entities within the framework, as also depicted in the figure, are as follows:

IT MANAGEMENT FRAMEWORK

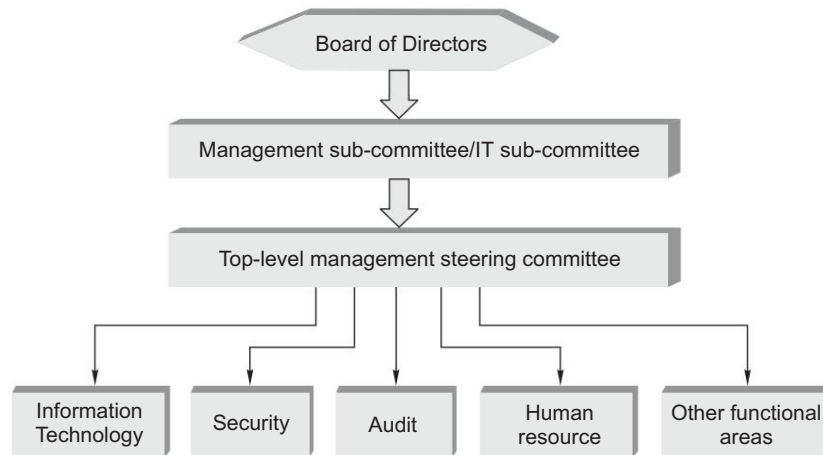


Fig. 4.1 IT Management Framework

Board of Directors

- Since a bank is a corporate entity, the board is responsible to the stakeholders
- The board must ensure that an internal control system or framework is in place
- At the board level, Information Technology should be considered from the management's perspective rather than as a purely technological issue
- Issues regarding the overall planning, budget, strategy, etc., related to Information Technology should therefore, be discussed preferably in the management-sub-committee of the board or if the bank desires in a separate IT sub-committee of the board
- Once the approval is obtained from the sub-committee, it should be brought only to the notice of the entire board for information

- The board should not engage itself in the operational matters of Information Technology. On operational matters, they should as far as possible, delegate the powers to executives or the executive-level committee
- While forming committees at various levels, it should be ensured that these have representatives from various important areas
- The board should ensure that the various developments in Information Technology, viz. the progress of various important projects, implementation of IT security policy, etc., are brought to its notice by the related sub-committee.
- Since Information Technology is a specialized subject, it is not expected of the board members, to be conversant with its nitty-gritty. Therefore, if required, they should engage the consultancy services of a reputed organization, having expertise in banking technology, to help them in matter related to IT
- The board should ensure smooth technology absorption in the bank. In this context coordination of IT department with various functional areas, viz. HR, IS Audit, legal, etc. is very important.

Board-Level Sub-committee

The basic rationale for a board-level sub-committee is that it will meet more frequently than the entire board and have very focused discussions on special issues. In our opinion, there need not be an exclusive board-level sub-committee for IT, the existing management sub-committee can discuss and take decisions on strategic issues related to IT. If there is a board member who is an IT specialist then he/she should also be a member of the management sub-committee. The broad areas which should be under the purview of the board-level sub-committee are as follows:

- Approving the strategic IT plan, with the business goal of striking an optimum balance of Information Technology opportunities and IT business requirements, as well as ensuring its further accomplishment
- Approving the IT budget, depending on the IT plan
- Reviewing project implementation at periodic intervals
- Approving the Information System security policy
- Discussing all other strategic issues like the decisions to opt for core banking or clustered banking, ASP model, strategic outsourcing, etc.

- Appraising the board about Information Technology issues
- In today's environment, it is not expected of the board members of the bank to be conversant with technology. Therefore, an expert, preferably from a reputed organization, with expertise, both in banking and technology may be consulted and if required the board may be asked to be an invitee in the sub-committee

Now, we think it important to mention, in brief what the board-level sub-committee should not routinely discuss:

- The details of an IT solution. For example, the board-level sub-committee can take a decision about whether or not to adopt core banking. But having decided that, details like the valuation of the vendor, preparation of RFP, etc., should be left to the executives
- While the Information Security policy needs the approval of the board, the lower level procedures and all other implementation issues should be dealt with by the executives
- On the basis of the strategic plan, approved by the board-level sub-committee, the short-term action plans can be prepared and finalized by the executives
- Any other operational issues related to Information Technology

Top Level Management Steering Committee

This committee is basically an operational committee which should meet more frequently than the board-level sub-committee and discuss/decide the following issues:

- Approval of action plan, based on the strategic plan
- Selection of generic solutions and the vendors
- Approval for Information System security procedures, which are based on the high-level organizational policy
- Implementation of IT solution
- If required, this committee can form specific, lower level, temporary committees for implementation of specific projects. These project teams should be, as far as possible, made cross-functional, with representation from user groups and all other relevant functional areas
- This committee should be headed by the Executive Director and can have members from various functional areas, viz. IT security, IS Audit, legal, HR, and any other important functional areas

Focused Work Areas

The following work areas should be considered as focus activity areas, for managing the Information System in an organization:

1. Information Technology Area

- IT policy and aligning IT strategy with business strategy
- Business technology planning process, including the sponsorship of collaborative planning processes
- New and existing application development for enterprise initiatives and overall coordination for business unit or divisional initiatives
- IT infrastructure and architecture, e.g. computers and networks, operations and investment decisions
- Sourcing and purchase decisions, which include 'make versus buy' decisions, relative to 'outsourcing versus in-house' provisioning of IT services and skills
- Establishing partnerships, including strategic relationship with key IT suppliers and consultants
- Technology transfer, by providing enabling technologies that make it easier for customers and suppliers to conduct business with the enterprise as well as increase revenues and profitability
- Interacting with internal and external clients to ensure continuous customer satisfaction
- Providing training to all IT users to ensure productive use of existing and new systems
- Implementing controls
- Managing day-to-day security functions

2. Information Security Area

- Communicate with the management about risks and controls, related to the Information System
- Ensure that appropriate user access and authentication controls are in place
- Ensure that the documented security policies, standards and procedures are reviewed, updated, and maintained periodically by appropriate individuals
- Evaluate security exposure, misuse or instances of non-compliance and ensure implementation of security controls to address these incidences

- Ensure that all business unit/departmental security coordinators understand and execute their security responsibilities in accordance with related policies, standards and procedures
- Organize and conduct, periodic security team meetings
- Develop and implement the security awareness program with assistance from security team members

3. Information Security Audit Area

- Audit planning
- Conduct reviews in accordance with established guidelines
- Develop audit reports
- Keep the management informed

The roles and responsibilities of various entities, mentioned in the above, proposed framework, are based on the industry standard and practices and are in no way exhaustive

Box 4.2

Plan Much Ahead of time

Way back in 1998, a commercial bank in India, had a very ambitious plan of modernizing its operations. The long-term IT plan was drawn which envisaged the setting up of a corporate network, connecting 500 branches, out of a total of 2000 branches, in a span of two years and then deciding about implementing the core banking applications in the network in the third year and finally, in the last two years, rolling out core banking the application in the 500 (Five hundred) networked branches.

The networking of branches, across fifteen major cities went off smoothly and the bank, at the end of the third year, had a robust Wide Area Network. Before taking a decision on the core banking application in the third year, the CEO who had taken the initiative, retired from the services of the bank, and a new CEO came in. The priority changed and instead of selecting the core banking application, the bank opted for cost-cutting measures, as the profit was believed to have been eroded because of the huge expenditure incurred setting up the Wide Area Network. At the end of the fifth year, the bank's network remained a network, devoid of any application in it. Other banks, who took similar initiatives, that too much later, were able to launch various IT-enabled delivery channels and the profit of this bank was reduced further. What went wrong for the bank that took the initiative much before the other banks? What was the basic flaw in the planning process? What should the bank have decided first, the application or the network?

ROLE OF THE AUDITOR IN EVALUATING THE PLANNING PROCESS

An auditor's task is to collect and evaluate evidence, to assure the management that the planning process underway in the organization is as per the management's expectation and in tune with the business requirement. The Information System is unlikely to be effective or efficient in the absence of a high quality Information Technology plan. And effectiveness and efficiency have a direct relationship with maintaining data integrity, and safeguarding of assets. For example, poor planning could mean inadequate Information Technology resources and their inadequacy could become one of the reasons for diluting the controls on asset safeguarding, and maintaining data integrity.

The role of an Information System auditor, in evaluating the planning function has been outlined below:

1. To acquire an understanding of the business needs, by understanding the domain and then interviewing some functionaries associated with the planning process, viz. CEO, chief Information Technology officer, chief information security officer, officials in charge of Information System Audit (in the case an external Audit), members of the IT steering committee, and some important functionaries of the IT department and other functional departments
2. The purpose of the interview should be to ascertain their involvement in and concern for the planning process. Such an interview should not be probing in nature
3. The auditor can also administer some customized questionnaires to the officials involved in the planning process
4. Documents like the information security policy and procedures, the long and short-range IT plans, the minutes of the steering committee meetings, the regulatory guidelines on the subject, etc., are required to be seen by the auditor for commenting on the efficacy of the planning process
5. At this stage, the auditor should ensure that appropriate authorities have approved the documents. Like in case of a bank, the IT security policy should be approved by the board of directors of the bank
6. After obtaining the necessary evidence, the auditor should evaluate the same to ensure that the IT or business enterprise policies and procedures, provide for a structured planning approach
7. In the absence of the documents mentioned above, the auditor should observe the processes and map it to the standard practices in the

industry or to governance models like COBIT and find out the gaps

8. If the auditor is not satisfied with the degree of compliance with the existing policy, like if the auditor finds that the short-term operational plans are not consistent with the long-term plan, then it is necessary to conduct more substantive tests
9. Auditors are also required to benchmark the strategic IT plans against those of similar organizations or appropriate international standards or recognized industry best practices
10. A detailed review of the IT plans must be undertaken to determine if the known areas of weakness within the organization are being identified for making improvement, as part of the IT solutions, contained in the plans

At the end of this exercise, the auditors should be able to identify:

- IT failures to meet the organization's mission and goal
- IT failures to meet cost and time guidelines
- Missed business opportunities
- Missed IT opportunities
- Inadequate controls because of poor planning

ORGANIZING

Once the goals are earmarked in the strategic IT plan, the next step is gathering, allocating, and coordinating the resources needed to accomplish the goal. Let us assume that a banking organization in its IT strategic plan, has decided to implement a centralized banking solution in 200 (two hundred) of its branches in different cities across the country, within 2 years. Now, to accomplish this, the management should initiate a process to select the centralized banking application, float a request for the proposal, network the locations, etc. For successful implementation, it should also have proper manpower resources, with adequate training and also a proper business process re-engineering, done across the organization to ensure in effective absorption of new technology.

Any laxity in the organizing function by the management, will have a direct effect on the business goal. In the following section, we will discuss the various management level functions required to be practiced in the organization which will help in organizing the resources, in accomplishing the goals set out in the long-range IT plan.

Policies and Procedures

Policies and procedures of an organization, reflect the guidance provided by the management in developing controls for the Information Systems, and other related resources. Here, when we talk of policies and procedures, it is a reference to not only the Information System security policies and procedures, but also to policies and procedures, affecting the Information Systems (data, application, technology, facilities, and people).

Before discussing the specific policies and procedures affecting the Information System, we will discuss in generic terms, the fundamentals of policies and procedures and the differences between them.

Policies

Policies are high-level documents. They represent the corporate philosophy of an organization and reflect the strategic thinking of the senior management and the business process owners. There are broadly two approaches for developing policies for an organization:

- Top-down approach
- Bottom-up approach

In the case of top-down approach, the lower level policies, i.e. the policies of departments or divisions are derived from the central corporate policy. Such kind of an approach ensures consistency within the organization. The bottom-up approach of developing policies, causes the enterprise policy to be derived from the department level policies. This kind of an approach is cost-effective and is sometimes required for legacy organizations because in these organizations, the department level policies are already developed before the organization decides to have a policy for the whole enterprise. Such kind of a bottom-up approach is also easy to implement, as it has been in vogue for sometime and has been derived following a detailed risk assessment. The management's role in framing and implementing of policies is as below:

- It must create a positive control environment by assuming responsibility for formulating, developing, documenting, promulgating, and controlling the policies
- It should ensure that the policy reaches the target audience
- It should review the policy periodically
- It also has the responsibility to ensure the existence of a necessary framework for policy updation, at appropriate intervals

- It should ensure the coordination of various departments in implementing the policy
- Above all, the policy goals have to be achieved by the top-level management

Procedures

Procedures represent the detailed, operational documents, derived from the parent policy. In fact, there is a one-to-many relationship between policy and procedure. A single policy can have many procedures and it is for the organization to adopt specific procedures, depending on its needs and cost efficacy. Procedures, being operational documents are very dynamic and can change more frequently than the policies.

A sample of policy and its related procedures is given below, for a proper understanding of these.

Managing User Access Policy

Access to all systems must be authorized by the owner of the system and such access, including the appropriate access rights (or privileges) must be recorded in an access control register. Such records are to be regarded as highly confidential documents and safeguarded accordingly.

PROCEDURE

- In the event of any employee/consultant/vendor or any entity, requiring access to the IT Systems of the department, the departmental head who is considered the owner of the system, has to approve the request in the 'user creation and access rights' assignment form
- This form will include the name, designation, department, and all other particulars of the employee requiring access
- In case of vendors, the name of the vendor, name of the company, and all other particulars need to be mentioned in the form
- The time and purpose for which access is required should also be mentioned in the form
- The resources to which access is required, like, the name of the operating system, and name of the database management system and application, should be mentioned in the user creation and access assignment form

130 *Information System Audit and Assurance*

- The list of objects which needs to be audited should also be mentioned in the form
- The user will be required to give an undertaking, to abide by the security requirements of the organization, from time to time
- On getting the request form, duly signed by the head of the department, the system administrator will assign the resources
- The first password will be assigned by the administrator and the user is required to change the password in the first login
- The request form will be kept as a permanent record in safe custody by the system administrator

A sample copy of the user creation and access rights assignment form is appended in Table 4.1.

HUMAN RESOURCES POLICIES AND PROCEDURES, RELATING TO THE INFORMATION SYSTEM

Personnel Recruitment and Promotion

Appropriate personnel always act as a good preventive control for the organization. The management should therefore, implement and regularly assess the required processes to ensure that personnel recruitment and promotion practices are based on objective criteria and that they take into account the personnel's education, experience, and responsibility. These processes should be in line with the overall organizational policies and procedures. The management should ensure that knowledge and skill needs are continually assessed and that the organization is able to acquire a workforce that has the skills, which match those, necessary to achieve organizational goals. Some of the fundamental controls required for various policies, relating to human resources are as below:

HIRING

- A background check before providing employment is very important. This background check can be done, both, in a formal and informal way. The purpose of the background check is to ascertain, from a third-party source, the credentials of the candidate and his/her suitability for the job and the organization

Table 4.1 User registration form

The Model Bank		
User creation and access rights assignment form		
Owner:		
Tick whichever is applicable ☐ Creation ☐ Update ☐ Revival		Location
Name (Block Letters)		Employee No.
Designation:	Department	Login Name
Resource	Group linked	Authorised by
Windows NT/ 2000 domain		
Novell Server		
File server		
Internet		
E-mail		
Other IT resources (by name)		
Application	Profile linked	Authorised by
Name of the application		
Resource (Application/ OS)	List of objects to be audited	
Remarks/special instructions:		
Please contact system administrator for your password.		
Change Password Immediately!		
Location:	Date	
		Signature of Department Head
I agree to observe all precautions and security measures as recommended in the IT Security Policy and Procedures and all guidelines, issued from time to time in this regard. I will use the application systems as per the laid down procedures and will not attempt unauthorized access and changes to data. I will follow the guidelines on the use of Electronic mail and Internet services.		
Signature of user (with date)		
Note: The list of resources/ applications included here is indicative and can be modified on the basis of need.		

- The organization should enter into a confidential agreement with the prospective employee for maintaining the confidentiality of the organizational matter. A confidential agreement is a quasi judicial document and maximum care should be taken to draft it. Some of the fundamental things which should be remembered while drafting the agreement are:
 - (a) The agreement should be in tune with the laws of the country. In other words, nothing in the agreement should be contrary to the laws of the land
 - (b) This document should be concise and clear
 - (c) This document and any other employment agreement must be reviewed by a competent labor counsel, before use
- For ready reference, the checklist for drafting a confidentiality/ non-disclosure agreement are appended below:
 - (a) The first provision should be to define what constitutes confidential information. This is important because it forms the basis of what may become the subject of a dispute. Additionally, the agreement should state how such information is to be determined and disclosed. For instance, the agreement can state that the defined information is confidential only if it is in writing, or only if it is disclosed in writing or if it is marked “Confidential” by the owner, etc.
 - (b) Additionally, and perhaps of equal importance is that the agreement can define what is *not confidential*. Generally, information that was known to the recipient before it was so disclosed would not be considered confidential. However, it is critical for the agreement to establish certain parameters that will decide what constitutes “knowing” beforehand. For example, if such information was available in writing, before the date of the disclosure or if it was used in the recipient’s business, before the date of disclosure, this can be used to define “known”
 - (c) The agreement should also clearly state that the act of disclosing certain information does not serve to transfer any rights, of any kind, in or to the confidential information from the discloser and that all rights are reserved to the discloser
 - (d) In a related provision, the agreement should also state that no license to use the confidential material is granted, by the act of disclosure of information and that, that should be the subject matter of a separate agreement in which there is a royalty, etc.

- (e) Of course, the meat of the agreement should be the scope of limitations on use of the disclosed information. Is it to be limited to preventing disclosure only by the recipient or is the recipient also responsible for preventing disclosure by any third party? The agreement should state how and in what manner the recipient may use the confidential information and whether or not copies may be made of the same and if so, what should be done with the copies, when the agreement ends
- (f) Additionally, these agreements often contain provisions, prohibiting the recipient from hiring any of the discloser's employees, at least for some stated period of time. The rationale is that by disclosing this information, the discloser becomes vulnerable and should not be victimized due to his/her act of disclosure
- (g) The agreement should go on to provide that the discloser is not making any representations or warranties about the information, but is disclosing the same on an "as is" basis
- (h) There should also be a specific term for the agreement, one that is commensurate with whatever the transaction may call for in a given set of circumstances. The more complex the transaction, the longer the term of the agreement should be. However, and this is very important, the recipient must be bound to hold in confidence, the information provided, even after the term ends
- (i) Moreover, there should be provisions, setting forth the remedies available to the parties, mostly the discloser, in the event of a breach or threatened breach of confidentiality on the part of the recipient. These remedies should, of course, include injunctive relief. There should also be appropriate provisions dealing with the place, where the action may be taken
- (j) Finally, there should be some mechanism, established for the actual process of disclosing the information. If this is to be done on a one-time basis, then the information should be marked clearly as confidential. If it is to be done on a regular basis, over some period of time, then appropriate procedures should be set up to establish that when disclosed, the information shall be deemed covered by the agreement
- (k) Often, non-disclosure agreements are combined with employment agreements and the same provisions should apply in those cases as well. However, in the case of employment agreements, there are many other provisions that should be included in these

agreements. These provisions may relate to the employee's work status, rights to the employee's work, and so on. These provisions may also have implications, in terms of the definition of confidentiality

- (l) Conflict of interest agreement– Conflict of interest policies address situations and circumstances in which an employee's personal interests are or appear to be in conflict with the organization's interests. There are many different definitions of 'conflict of interest'. Often, definitions focus on the opportunities that an employee may have to use his/her position in the organization, to his/her personal advantage or to the advantage of friends or family members. From a control perspective, the organization's policy needs to have a clear statement, defining conflict of interest that suits the organization's purposes. It should also assign responsibility for identifying and resolving actual and potential conflicts. While some policies do not spell out the consequences and the likely effect on an employee, if a conflict cannot be resolved, others specify that the failure to resolve a conflict of interest will result in disciplinary action or termination of services
- (m) Non-compete agreement– A non-compete agreement can be used to prevent former employees of a company from competing against it after they have left the company. This form allows an employer to draft an agreement that may keep an employee from:
 - Leaving in the first place
 - Defecting to a competitor
 - Opening a competitive business concerns
 - Disclosing company secrets
 - Soliciting the company's customers, clients, and employees

These non-compete agreements are sometimes expressly declared as void, by the laws of some countries. For example, in India, as per the India Contract Act, agreements in restraint of trade are expressly declared as void. Therefore, care should be taken to take the laws of the country into consideration while framing the non-compete agreement.

Some points related to control which should be taken care of while hiring are as below:

- Proper care should be taken while hiring third party and contractual employees

- For very important and sensitive positions, the organization should employ regular employees instead of part-time or contractual staff
- Extra care should be taken before recruiting frequent job-changers

PROMOTION OF PERSONNEL

The management should implement and regularly assess the required processes to ensure that the practices of personnel promotion are based on objective criteria and that take into account, the employees, education, experience, and responsibility. These processes should be in line with the overall organizational policies and procedures in this regard, such as hiring, orienting, training, evaluating, counseling, promoting, compensating, and disciplining. The management should ensure that knowledge and skill needs are continually assessed and that the organization is able to acquire a workforce that has the skills, which match those necessary to achieve organizational goals.

PERSONNEL TRAINING

The management should ensure that employees are taken through an orientation program upon hiring, and provided on-going training, to maintain to level of their knowledge, skills, abilities, and security awareness required to perform effectively. Education and training programs, conducted to effectively raise the technical and management skill levels of the personnel should be reviewed regularly.

CROSS-TRAINING OR STAFF BACKUP

The management should provide for sufficient cross-training or backup of identified, key personnel to address problems of unavailability of employees. It should establish succession plans for all key functions and positions. Personnel in sensitive positions should be required to take compulsory, uninterrupted holidays of sufficient length to test the organization's ability to cope with unavailability of personnel, and to prevent and detect fraudulent activity.

Cross-training involves the risk of a single person knowing all parts of the system. The management should be aware of this risk.

EMPLOYEE JOB PERFORMANCE EVALUATION

The management should implement an employee performance evaluation process, reinforced by an effective reward system that is designed to help

employees understand the connection between their performance and the organization's success. Evaluation should be performed against established standards, and specific job responsibilities, on a regular basis. Employees should receive counseling on performance or conduct whenever deemed necessary.

JOB CHANGE AND TERMINATION

The management should ensure that appropriate and timely actions are taken regarding job changes and job terminations, so that internal controls and security of the organization are not impaired by such occurrences.

One of the best practices followed now, across organizations, is preparing an employee handbook, which can be called by any other fancy name like "Know thy organization", etc. It serves as an important source of information for employees, about the policies and procedures regarding human resources. Such a handbook should contain:

- The expectations of the organization
- The abstract of the security policy
- Performance evaluation
- Emergency procedures
- Disciplinary actions for breach of policies and procedures, etc.

OUTSOURCING PRACTICES

Companies elect to outsource for a variety of reasons, some strategic and others tactical. In the past, outsourcing has often been used tactically, as a rapid and often short-term solution to a particular need or problem, which does not form part of the overall business strategy.

Such kind of arrangements can be called out-tasking instead of outsourcing. The outsourcing which we will be discussing here, is essentially strategic outsourcing, which means that an organization works with one or more supplier/company in order to bring about a significant long-term improvement in business performance. This is a contractual agreement, whereby, the organization hands over control of a part or all functions of a particular work area to an external party. As a practice, it has existed for decades, but it has seen a revival in recent times, driven by the desire of companies to focus on core competencies, the need for speed, and the imbalance between or shortage of manpower and the right skills. According to the Outsourcing Institute, USA, outsourcing is defined as, *'the procuring of services or products from an outside supplier in order to reduce costs, fill the gap of (or replace) in-house*

capabilities and minimize time scales of projects, without the loss of control or flexibility'.

From the control perspective, an auditor should be aware of various reasons for outsourcing, its advantages and disadvantages, and also the control requirements of outsourcing the Information System functions.

Why Outsourcing?

There is growing popularity of adopting a strategic approach to outsourcing. This stems from the simple fact that organizations adopting this method, appear to do well. Strategic outsourcing is only likely to be effective and bring the desired results, if the management is prepared to adopt a completely new perspective on management control. Organizations are more likely to meet their commercial objectives and maximize their success, if they direct the management control not so much towards controlling inputs, but towards focusing on the finished output. The feedback given on the output, by the management, will automatically become an input and these inputs become more effective if the management's feedback on output is focused and objective.

The various reasons for embarking on outsourcing are:

- To reduce and control the operating costs
- To improve the focus of the organization
- To gain access to world-class capabilities
- Lack of internal resources
- To accelerate the benefit of re-engineering
- Functions difficult to manage/out of control
- To make capital funds available
- To share risks
- Cash infusions
- Redirect resources for other purposes

Reduce and Control the Operating Costs

Organizations that try to do everything by themselves, may incur high research, development, marketing, and deployment expenses, all of which then are passed on to the customer. An outside provider's lower cost structure, which may be the result of greater economy of scale or other advantages, based on specialization, reduces the organization's operating costs, and increases its competitive advantage.

Improve the Focus of the Organization

Outsourcing lets an organization focus on its core business activities allowing its having operational functions to be assumed by an outside expert. Freed from devoting energy to areas that are not its expertise, the organization can thus, focus its resources on meeting its customers' needs.

Gain access to World-Class Capabilities

World-class providers make extensive investments in technology, methodologies, and people. They gain expertise by working with many clients, facing similar challenges. This combination of specialization and expertise gives customers a competitive advantage and helps them avoid the cost of chasing technology and training. In addition, there are better career opportunities for personnel who make the transition to an outsourcing provider.

Lack of Internal Resources

Companies outsource because they do not have access to the required resources within the company. Outsourcing is a viable alternative to building the needed capability within the organization from scratch. New organizations, spin-offs, or companies expanding into newer geographical areas or new technology should consider the benefits of outsourcing from the very beginning.

Accelerate the Benefits of Re-engineering

Re-engineering aims at bringing about dramatic improvements in critical measures of performance such as cost, quality, service, and speed. But the need to increase efficiency can come into direct conflict with the need to invest in core business. As non-core, internal functions are continually put on the back burner, systems become less efficient and less productive. By outsourcing a non-core function to a world-class provider, the organization can begin to see the benefits of re-engineering and the outsourcing partner becomes an agent of change for the organization.

Functions Difficult to Manage/Out of Control

Outsourcing is certainly one option for addressing this problem. It is critical to remember that outsourcing doesn't mean abdication of management responsibility nor does it work well as a knee-jerk reaction by a company in trouble.

When a function is viewed as difficult to manage or out of control, the organization needs to examine the underlying causes. If the requirements, expectations, or needed resources are not clearly understood, then outsourcing

won't improve the situation; it may in fact, exacerbate it. If the organization doesn't understand its own requirements, it won't be able to communicate them to an outside provider.

Make Capital Funds Available

There is tremendous competition within most organizations for capital funds. Deciding where to invest these funds is one of the most important decisions that the senior management has to make. It is often hard to justify non-core capital investments, when areas more directly related to producing a product or providing a service are competing for the same money.

Outsourcing can reduce the need to invest capital funds in non-core business functions. Instead of acquiring the resources through capital expenditures, they are contracted on, an "as used" operational, expense basis. Outsourcing can also improve certain financial measurements of the firm by eliminating the need to show Return On Equity from capital investments in non-core areas.

Share Risks

Tremendous risks are associated with the investments an organization makes. Markets, competition, government regulations, financial conditions, and technologies, all change extremely quickly. Keeping up with these changes, especially those in which the next generation requires a significant investment, is very risky.

Outsourcing providers make investments on behalf of many clients, not just one. Shared investment, spreads the risk and significantly reduces the risk borne by a single company.

Cash Infusion

Outsourcing often involves the transfer of assets from the customer to the provider. Equipment, facilities, vehicles, and licenses used in the current operations have value and are sold to the vendor. The vendor then uses these assets to provide services to the client. Depending on the value of the assets involved, this sale may result in a significant inflow of cash payment to the customer.

When these assets are sold to the vendor, they are sold at book value. The book value can be higher than the market value. In these cases, the difference between the two actually represents a loan from the vendor to the client, which is repaid as services, over the life of the contract.

Redirect Free Resources for Other Purposes

Every organization has limits on the resources available to it. Outsourcing permits an organization to redirect its resources, most often human resources, from non-core activities toward activities which directly serve the customer. The organization can redirect these people or at least the staff slots they represent, to greater, value-adding activities. People whose energies are currently focused inwards, can now be focused outwards— on the customer.

What to Outsource?

From the discussion above, while the objectives or whys of outsourcing can be easily explained i.e. lower costs, improved effectiveness, better service levels, increased reliability, access to better skills, etc. it's another story altogether, when it comes to thinking about what to outsource. Here are a few factors to consider, when you study the suitability of IT functions and processes that can be outsourced.

How Standardized and Stable are the Set of IT Processes in Question?

Can the processes be easily automated or standardized? The general rule is that if the process is largely procedural or can be easily repeated (such as installing upgrades or performing a virus scan), then it lends itself to outsourcing. Standardization reduces complexity and costs. However, if nobody, except an expert like Mr X can or should perform the process, then you should probably reconsider the decision to outsource such a process.

Do You Have Problems Acquiring Skilled Resources?

It goes without saying that the better the skills, the better will be the results. However, even the best IT personnel in the market may not be willing to work in a supporting department, within your organization. For an outsourcing services provider, the IT profession is the core; therefore, it is more likely to invest in training, pay competitive salaries, and provide for the requisite development, required to retain these skills. In addition, the best practices and knowledge obtained, by dealing with many companies, make the service provider uniquely enabled to keep your IT processes up and running, more reliably with improved customer satisfaction.

Is Your Business Inherently Dynamic?

Companies with a need to respond dynamically to volatile changes, unpredictable growth, or seasonal, but predictably heavy workloads, may find that an outsourced IT model works much better, than investing in minimum infrastructure that is necessary to cope with business peaks, which may come only once a year. For example, if your system runs out of capacity during a particular successful marketing campaign, you would traditionally have to buy, install, and allocate the requisite amount of additional capacity which could take up to six weeks, by which time the business peak and opportunity may have already passed. A more viable alternative would be to outsource IT processing, so that capacity requirements can automatically be provided for, when needed, that too in a matter of hours, if not minutes.

Does the Performance of This Activity Represent a Core Competency of the Organization?

If the process or activity is not one of the core activities of the company, then it does not make sense to engage the intellectual capital of the company into such an activity. This will be as good as missing the forest in the quest for individual trees.

In fact, IT processes can be broken down into various activities and three questions asked in respect of each activity. A negative answer to any of the three questions, may provide the case for outsourcing:

- Does the performance of this activity represent a core competency of the organization?
- Does the performance of this activity support the strategic direction of the organization?
- Can the organization perform this process at a lower cost, with a better quality of results?

Considering the above, the under-mentioned activities of the Information System function can be outsourced:

- Data entry
- Design and development of new applications, when in-house staff does not have the necessary expertise or they are busy with other important work
- Maintenance of new applications, when in-house staff are developing new applications
- Conversion of legacy applications to new platforms (when there is no in-house expertise to do that)

142 *Information System Audit and Assurance*

- Help desk or call center
- Data center operations
- Backup and recovery
- Performance tuning and management
- Capacity management
- Credit card processing
- ATM cash replenishment
- Language translation
- Documentation

The advantages and disadvantages of outsourcing have been outlined appended in the table below.

Table 4.2 Advantages and Disadvantages of Outsourcing

<i>Advantages</i>	<i>Disadvantages</i>
Outsourcing vendors can achieve economy of scale by deploying reusable components.	Cost may exceed customer expectation.
Outsourcing companies give more attention and focus to the work which is their source of income.	The organization should have a contingency plan, in case of failure of the third party to perform assigned activities.
Reduction of cost of operations.	Fear that the supplier will settle for a lower quality of technology for reducing expenses.
Ability to accurately forecast computerization budget.	Fear of losing control over information resources and dependence on the service provider.
Dividing up the computerization budget (funding).	Fear of a leak of sensitive information.
No problems like workers unions striking and halting computer operations.	Fear of key system personnel leaving during the process.
Possible to build a highly efficient computerized department.	Worries about the supplier's stability and survivability.
Construction of a measurable level of service and improved service to the organization and clients.	Lack of control over service levels, possible detrimental effect on service to clients.

(Contd)

<i>Advantages</i>	<i>Disadvantages</i>
The act of developing specifications and contractual agreement for outsourcing services is likely to result in better specifications, than if developed only by and for in-house staff.	“Transitional phase”– a period in which there is a significant danger to the organization's operations.
Efficient management of computer equipment assets.	Fear of its being a “one-way street”, with no way back to the beginning.

The Selection Process of Outsource Vendors

Since outsourcing is a strategic decision, the selection of outsource partners requires careful consideration. The following steps are critical to making an informed choice about selection of an outsource vendor:

- Know what you are seeking and why. You should not undertake the exercise of vendor selection, until you have clearly identified the business processes/activities that you are seeking to outsource (the what) and the benefits or advantages you are seeking to achieve through outsourcing these (the why)
- Involve all stakeholders in an evaluation team. The team should include representatives of those parts of the organization with a stake in the success of the process under consideration. Care should be taken to ensure that there is adequate representation from the functional areas.
- Clearly define and communicate your requirements in an RFP. The Request For Proposal (RFP) that you issue to potential outsource vendors should clearly define all requirements related to the business process to be outsourced. ‘Right to audit’ should be specifically mentioned in the RFP
- Prepare a vendor shortlist. Evaluate vendor responses to your RFP, against defined criteria, to eliminate those vendors who are less likely than the others to provide you optimal satisfaction
- Evaluate the shortlisted vendors, thoroughly. The evaluation process has been discussed below:
- Select a service provider. Based on your evaluation, identify the vendor that provides the most promising solution to your problems and requirements.

- Negotiate a service-level agreement. Now, you are ready to negotiate the contract to govern your relationship with the selected outsourcer

Evaluating Outsource Partners

Outsourcing is not only a cost decision, it is a strategic decision that has significant control implications for the management. Quality of services, assurance for continuity of services, financial viability, technical and domain expertise are the important issues that need to be evaluated for selecting an outsource partner. Choosing the right supplier is extremely important, particularly when outsourcing is a long-term strategy. The compatibility of suppliers in terms of culture and personnel is also an important issue, not to be overlooked by the management.

The following criteria should be considered during the evaluation process:

- **Methods:** Does the vendor employ methods for performing the business process in question, that meet or exceed industry standards, and that are also consistent with your business requirements?
- **Management:** Does the vendor have in place, a management team that is capable of delivering the service agreed upon, while also being able to handle any contingency that may arise in its own business environment?
- **Business domain knowledge:** Does the vendor have the requisite experience and knowledge about your industry and the ability to meet business requirements, similar to your own? Can the vendor bring to bear experience that may be applied to devise improved solutions for you?

Prepare a vendor short list. Evaluate vendor responses to your RFP, against defined criteria, to eliminate those vendors who are less likely than the others to provide you optimal satisfaction.

- **Tools and technology:** Does the vendor have in place the technology environment to support world-class service delivery? Does the vendor have a strategy for maintaining state of the art technology and the skills to operate it?
- **Financial viability:** Is the vendor financially stable? Is there a reasonable assurance that the vendor will be around to fulfill the terms of your service agreement?
- **Pricing, terms, incentives, and warranty:** Are the vendor's pricing and other terms competitive? Do they provide a satisfactory cost/benefit

business case for your firm? Is the vendor willing to negotiate incentives and penalties based on performance? Is the vendor's work warranted?

Strategies in Audit of Outsourcing

An organization that has outsourced a part of its Information System operation, would want an independent, third-party assurance, from an auditor, that the outsource vendor is taking care of all the control requirements, which also include issues related to confidentiality, availability and integrity of data. This third-party auditor should be acceptable to both the parties and must be agreed on, upfront.

In some activities, like outsourcing the data center, the organization that has outsourced its operation, would be concerned about the security and control at the vendor's site, where important data of the organization are stored. The control issues in such arrangements are:

- Physical access control
- Control at the gateway, i.e. where links of various other customers terminate
- Access to the access control data, pertaining to the particular company, etc.

To address various control issues, related to outsourcing services, the Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, an internationally recognized auditing standard, was developed by the American Institute of Certified Public Accountants (AICPA). An SAS 70 audit or examination is widely recognized, because it indicates that a service organization has been through an in-depth audit of their control activities, which generally includes, controls over Information Technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards, when they host or process data belonging to their customers.

SAS No. 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and also to their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report, including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of the SAS 70 examination.

Box 4.3**Who is the ultimate gainer?**

A proactive government bank, in the year 1992, decided to go in for credit card operations. At that time, barring a few foreign banks, no government-owned bank had even thought about it. The launch of the credit card operations created lots of hype in the market and the bank's customer base also increased. However, the product was an IT-enabled one and there was no sufficient or appropriate Information System available in the bank, to support it. Consequently, the claim for the transactions, made by the customers, using the credit cards were reaching them after 6 to 7 months of the transactions. The customers were enjoying. As a result, a proactive effort, which added to the customer base of the bank, also added to the Non-Performing Assets (NPA) of the bank. Ultimately, the bank had to write off a huge outstanding and give a contract to another IT firm for reconciling the balances of the credit card transactions. So what was wrong in the planning process?? Who is to be blamed for this??

ORGANIZATION OF INFORMATION SYSTEM AREA

In placing the IT function, in the overall organizational structure, the senior management should ensure authority, critical mass, and independence from the user departments, to the degree, necessary to guarantee effective IT solutions and sufficient progress in implementing them, and to establish a partnership relation with the top-level management, to help increase awareness, understanding and skills in identifying and resolving IT issues.

Should there be a separate Information System department or not? If a separate department is created, then should it have a centralized or decentralized set up? These are the questions, which have traditionally been the area of discussion in the industry. The decision to either have a separate Information System department or not, depends on how much the organization is dependent on the Information System. The more the organization depends on the Information System, the stronger is the case for having a separate Information System department. As regards, whether the setup should be centralized or not, it essentially depends on the type of the organization. If the decision-making in the organization is centralized, then it is always advisable to have a centralized Information System department.

Traditionally, an Information System department would have a system development group, a programming group, an operation group, a data

preparation group, and a general support or control group. These groups are further divided into sub-groups, depending on the requirements of the department. For example, the data processing group can take charge of areas like system analysis, programming, operation, etc. Over the years, with the advancement of Information Technology, the role of the Information System department has undergone a paradigm shift. Much of the activities, like data preparation, data entry, etc. have been entrusted to the user department. Whatever be the areas and the sub-groups in the IS department, the most important control requirement is an appropriate segregation of duties, with minimal conflict of interest. The senior management should implement a division of roles and responsibilities, which should ensure that the possibility of a single individual, subverting a critical process is completely eliminated. The management should also make sure that personnel are performing only those duties, stipulated for their respective jobs and positions. In particular, a segregation of duties should be maintained in respect of the following functions:

- Information Systems use
- Data entry
- Computer operation
- Network management
- System administration
- Systems development and maintenance
- Change management
- Security administration
- Security audit

A *separation control matrix*, depicting the possible role clashes of various Information System areas is given in Table 4.3.

The role clashes mentioned above, are generic and there seem to be no appropriate compensatory control if the conflicting roles are combined.

Now, let us discuss likely organizational setup of the Information System department of a banking organization. Considering the present scenario and future prospects, our target banking organization, will have the following attributes:

- Either Central Banking Solutions (CBS) already implemented or in the process of implementation
- Apart from the CBS branches, most of the branches are fully computerized with an independent application, working in a Local Area Networking (LAN) environment

Table 4.3 Separation of duties control matrix

	System analyst	Application programmer	Data entry	Computer operator	Database administrator	Security administrator	Quality assurance	Network assurance	System assurance
System analyst			x	x	x	x	x	x	x
Application programmer			x	x	x	x	x	x	x
Data entry			x	x	x	x		x	x
Computer operator	x	x	x		x	x		x	x
Database administrator	x	x	x	x				x	x
Security administrator			x	x	x	x			
Quality assurance	x	x						x	x
Network administrator	x	x	x	x	x		x		
System administrator	x	x	x	x	x		x		

- The bank has an ambitious plan of wide area networking, more delivery channels like internet banking, ATM switch, etc.
- The bank has a centralized Information Technology division

First and foremost, in devising the organizational set up for the Information Technology department, the work areas inside the IT division need to be defined. After defining the work areas, these should be assigned to their respective locations.

The locations and required Information System activities in those locations are depicted in the matrix below.

Table 4.4

	Data center	CBS branches	TBA branches	Information Technology division	Training establishments
Networking	✓			✓	
Software development				✓	✓
Testing and quality assurance				✓	
Backup/restore/achieve	✓		✓		

(Contd)

	<i>Data center</i>	<i>CBS branches</i>	<i>TBA branches</i>	<i>Information Technology division</i>	<i>Training establishments</i>
Delivery channels				✓	
Policy/planning and MIS				✓	
Database administration	✓		✓		✓
System administration	✓	✓	✓		✓
Hardware and software acquisitions				✓	
Information Technology security	✓	✓		✓	
Help Desk	✓			✓	

Based on the 'function-location' matrix and the 'separation of duties' matrix, an indicative organizational structure for each location has been depicted shown in Fig. 4.2.

LEADING

Evaluating the effectiveness of the leading function of the management is a difficult task and more so, when done by an Information System auditor. The question people sometimes ask is, whether this falls within the purview of Information System Audit at all. Even Information System auditors find it difficult to evaluate the top-level management's ability to lead people. But the fact is that an Information System will remain ineffective, in the absence of effective leadership and therefore, an IS auditor cannot absolve his/her responsibility in this area. After all, he/she is responsible for assuring the management that the Information System is safeguarding assets, maintaining data integrity, fulfilling organizational goals effectively, and consuming resources efficiently.

For effectively discharging their duty of evaluating the leading functions of the top-level management, the IS auditors should have a basic understanding of the fundamentals of effective leadership, motivating subordinates, and communicating clearly with them.

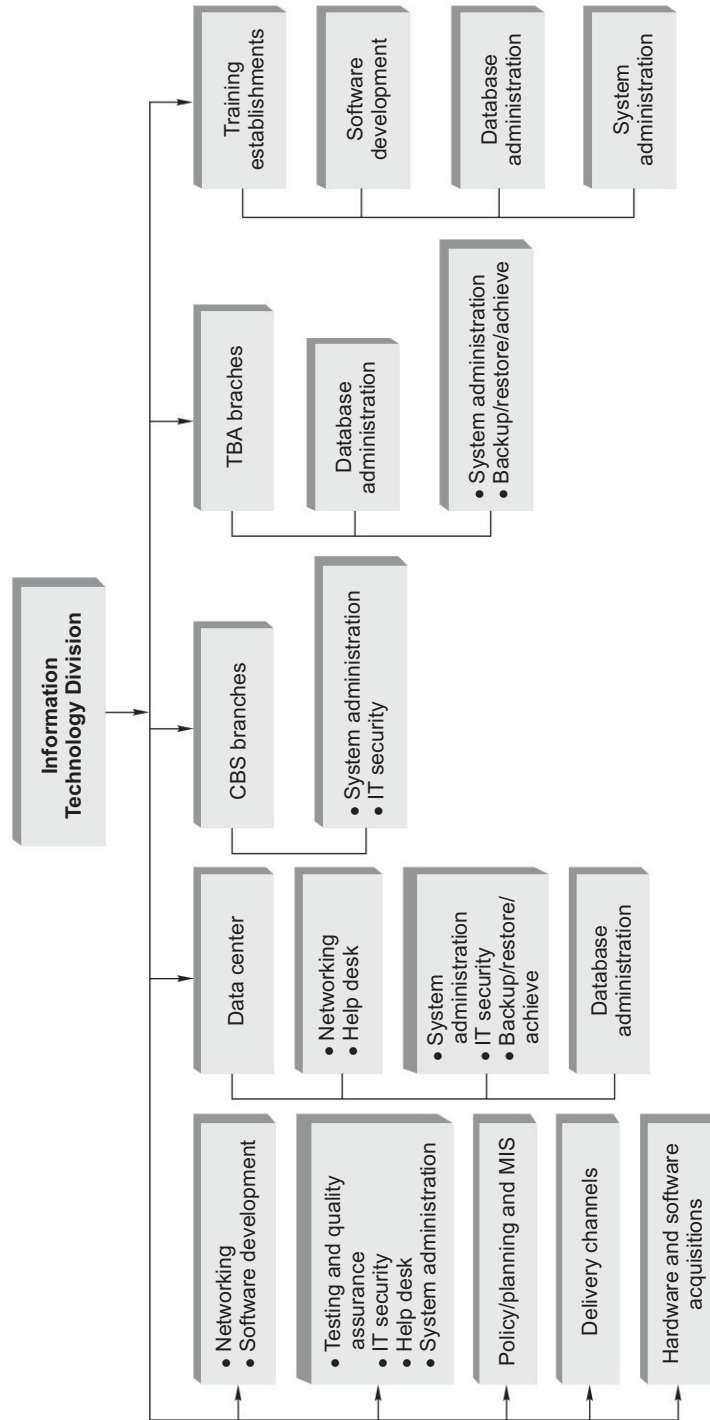


Fig. 4.2 Organizational Structure for Information Technology Division

From an auditor's perspective, it is very important to be aware of some of the objective indicators that suggest poor leadership, viz. staff turnover, projects failing to meet budget limits, the growth/profitability, number of officials trained, post-training review, assessment and deployment, etc. These parameters, although necessary are not sufficient to reach any conclusion. Therefore, the auditor should also interview staff members and top officials, in order to collect and evaluate subjective evidence. Both objective and subjective evidence can be used by the auditor to give an opinion about the effectiveness of the leadership function of the management. Documents like the Information System plan, Information Technology security policy, the minutes of the steering committee, some important office notes which may have been put up to the top-level management, for approval of IT projects, can also be of great help to the auditor.

CONTROLLING

From the management's perspective, controlling the Information System, concerned more with controlling the output rather than the input. Since the input of a system is always based on the feedback given by the output system, the management performs the job of supplying the necessary feedback for further input for the system and this feedback is based on an evaluation of the output. Therefore, controlling the output is more important from the management's point of view. For example, a help desk system forwards complaints to the top-level management if these are not resolved within 72 hours. On seeing the number of complaints and their degree of importance, however, the management decides that complaints should be forwarded to them, if not resolved within 24 hours and not 72 hours. This feedback is based on the output and accordingly, the help desk system is modified.

Broadly, there are two resources, viz. financial and human, where management control is very important from an Information System perspective. The pertinent questions in the mind of the management about these two resources are:

- How much should the organization spend on the Information System?
- What about the Return On Investment on the Information System?
- What controls over the activities, undertaken by the Information System personnel, are in place?

How Much should the Organization Spend on the Information System?

In an organization, where most of the work processes are computerized and there is fairly, sufficient IT absorption across the organization, the most frequently deliberated thought, among the management is how to control IT spending. The deliberations often shift focus from the question of “how to control the spending on IT?” to the question of “how to reduce the expenditure on IT?” Rarely does the management think about “how to control the investment in Information Technology?”

One way of controlling investment in IT, adopted by many organizations, is to benchmark this to a similar industry and compare. This, we call, the neighbor’s effect or demonstration effect. Such kind of a strategy is a reactive rather than a proactive approach. The organization continues to follow that actions of other organizations and thus, is unable to reap the benefits that come with making the first move. This reflects that the management still views Information Systems as a back office function, rather than one that might be central to the accomplishment of the corporate mission. Such kind of a view of the management, reflects that it sees the Information System function as an expenditure rather than an investment.

Another prudent way for controlling investment in Information Technology is having a framework, based on a balanced business scorecard (The Balanced Business Scorecard— Measurements that Drive Performance, Robert S. Kaplan and David P. Norton, Harvard Business Review, January-February 1992), where there are Critical Success Factor (CSF) which define the most important issues or actions for the management, to achieve control over and within its IT processes. CSF must act as a management-oriented, implementation guidelines and should identify the most important things to do, strategically, technically, organizationally, or procedurally.

Key Goal Indicators (KGI), which define the measures that tell the management— after the fact— whether or not an IT process has fulfilled the business requirements and Key Performance Indicator (KPI), which defines measures that determine how well the IT process is performing, in facilitating the achievement of the goal; are lead indicators that tell whether or not a goal is likely to be achieved. They are good indicators of capabilities, practices, and skills.

The management guidelines of COBIT, have already taken this balanced business scorecard into consideration and described the Critical Success Factor (CSF), Key Goal Indicator (KGI) and Key Performance Indicator (KPI), for control of IT investment by the management. The description of each of these can be accessed at www.isaca.org.

For the readers convenience, we have reproduced these below:

CRITICAL SUCCESS FACTOR (CSF)

- All IT-related costs are identified and classified
- An effective IT asset inventory that facilitates accurate cost measurement is maintained
- Formal investment criteria are defined for decision-making, in a responsive approval process, adaptable to the type of project under-way
- An IT delivery plan is defined, providing context, so that a clear view exists of on-going work and investments, technology lifecycles, and technology component reusability
- An investment decision-making process is defined, which also considers among others, short and long-term effects of investment, cross-divisional impact, business justification, benefit realization, strategic contribution, and compliance with the technology architecture and direction
- To allow for clear choices based on impact, measurable benefits, time-frames, and feasibility, investment decisions need to be presented with options and alternatives
- IT budgets and investments are aligned with the IT strategy and business plans
- Authority for expenditure approval is clearly delegated
- Budgets that cover end-to-end expenditures have identifiable and accountable owners, are time bound and closely tracked in an automated manner
- There is clearly defined management accountability for realizing forecasted benefits and a process to track and report the realization of benefits exists, thus, eliminating cross-subsidies
- There is clearly defined management accountability for realizing and tracking forecasted benefits
- Decision makers consider the full impact, including the complete lifecycle and adverse effects on other business units

KEY GOAL INDICATOR (KGI)

- Percentage of IT investments, meeting or exceeding expected benefits, based on Return On Investment and user satisfaction

154 *Information System Audit and Assurance*

- Actual IT expenses as a percentage of total organizational expenses vs. target
- Actual IT expenses as a percentage of revenues vs. target
- Percentage of business owner IT budgets that have been met with
- Absence of project delays, caused by lags in investment decisions or unavailability of funding

KEY PERFORMANCE INDICATOR (KPI)

- Percentage of projects, using the standard IT investment and budget models
- Number of months since the last review of budgets
- Time-lag between deviation occurrence and reporting
- Percentage of project files containing investment evaluations
- Number of projects where business benefits are not verified post-facto.
- Number of projects revealing investment or resource conflicts, after approval.
- Number of instances and time-lag, in delayed use of new technology.

What Controls Over the Activities, Undertaken by the Information System Personnel are in Place?

The activities of the Information System personnel cannot be controlled by maintaining a close watch on their activities, on a day-to-day basis. The best and probably the only effective way to have control over their activities, is through the establishment and enforcement of policies, procedures, and standards. While policies are high-level documents, procedures are detailed operational documents. These serve as a very useful tool for the management, in controlling activities of the Information System personnel, as per the accepted standards.

AUDITING MANAGEMENT CONTROL ON THE INFORMATION SYSTEM

From an auditor's perspective, auditing the management control on the Information System is basically a sort of 'effectiveness' audit. The steps required to be followed by the auditor for conducting an effectiveness audit of the management subsystem of the Information System are as follows:

- At the planning stage, the auditor should make him/herself aware of the inherent risks of the particular industry he/she may be associated with, by reading industry-related literature
- The relevant government and regulatory guidelines should be read and understood by the auditor
- The engagement letter to be made by the auditor, should be very specific about the audit. It would also be a good idea for the auditor to mention in the engagement letter that during the audit, it will be necessary to interview some top-management functionaries, including the CEO
- The auditor should follow the four-prong approach given by COBIT, i.e. obtaining, evaluating, assessing, and substantiating
- The 'obtaining' phase will be a combination of conducting interviews with officials and going through documents
- For auditing a management control framework, the auditor needs to interview the following officials:
 - Chief Executive Officer (CEO)
 - Chief Information Technology Officer (CITO)
 - Chief Information Security Officer (CISO)
 - Chief of Information System Audit (internal audit)
 - Important functionaries of the Information System department
 - The members of the steering committee
- The following documents need to be reviewed by the auditor:
 - Senior management plan/steering roles and responsibilities
 - Organizational objectives and long and short-range plans
 - IT objectives and long and short-range plans
 - Organization chart, showing the IT function in relation to other functions
 - Policies and procedures, related to the IT organization and relationships among organizational units
 - Policies and procedures, related to quality assurance
 - Policies and procedures, used to determine the IT staffing requirements
 - IT function organization chart
 - IT function, roles and responsibilities
 - IT function, key position (job) descriptions
 - Status reports and minutes of planning/steering committee meetings

- The previous audit reports
- The various documents reviewed should be further assessed to determine, whether or not they have been prepared as per the management's authorization and as intended by the management and also if they are current and up-to-date
- The IS auditor should also observe the actual functions carried out by the Information System personnel, in order to ensure that the individual who is assigned and authorized to perform a particular function, is the person who is actually doing the job. It allows the auditor to see, whether or not policies and procedures are understood and practiced across the organization
- After obtaining the evidence, the auditor should conduct the evaluation. At this stage, the auditor can use the customized check list given below:
 1. Depending on the score, the auditor should decide whether or not, to go for more substantive tests
 2. If there is a help desk system where complaints get forwarded to the top-management, if not resolved within 24 hours, the auditor should register a complaint, and ensure that it does not get resolved and then observe the reaction of the top-management, when it reaches them
 3. The auditor should also evaluate the projects undertaken and find out whether these are as per the long-term plan or not. If not, then the auditor should look for the top-management's approval, for taking up these projects
 4. For high-priority projects, the auditor should see, how often the management discusses the issues regarding the successful completion of these projects, in the steering committee
 5. For projects which have been delayed, the auditor should find out what exactly went wrong, with a special emphasis on the adequacy of management controls in such projects
- Some of the significant indicators of potential problems in the Information System function are:
 - High staff turnover
 - Frequent hardware/software errors
 - Delayed projects
 - Excessive backlog of user request
 - Numerous aborted or suspended development projects
 - No structured purchase of hardware and software

- Frequent hardware and software upgrades
- Extensive exception reports
- Lack of succession plan
- Poor motivation
- Excessive reliance on one or two key personnel

Auditing management control of Information System is a difficult task, especially since the auditor will be required to deal with the top-level management and give some remarks about the efficacy of management control.

The checklist given below is just indicative. Since, in the view of the authors, a “Yes” and “No” checklist for audit, is not a true audit/control exercise, a score based approach has been used, where each question is given a score, which ranges from 1 to 4. Depending on the scores in the relevant areas, the total score of the organization is arrived at as below:

Checklist for Auditing the management control framework of the Information System function

A. Planning

1 = Unclear, 2 = Somewhat unclear,

3 = Fairly clear, 4 = Clear

1. Is there a documented, long-term Information Technology plan? (4 = Yes; 1 = No)	1	4			
2. If it exists, has it been approved by the Top-level management? (4 = Yes; 1 = No or the answer to question number 1 4)	1	2	3	4	
3. Does the plan cover the following?	1	2	3	4	
• Existing and proposed hardware and network- ing architecture for the bank and its rationale					
• Broad strategy for procurement of hardware, software solutions, vendor development, and management					
• Standards for hardware and software, pres- cribed by the proposed architecture					
• Strategy for outsourcing, in-sourcing, pro- curing off the shelf software, and in-house development					
• Information security architecture					
• IT department's organizational structure					

(Contd)

158 *Information System Audit and Assurance*

• Desired level of IT expertise in banks, human resources and a plan to bridge the gaps between the two, if any • Strategies converted into clear IT initiatives, with a broad time frame • IT costs and cost management • Plan for transition, if any				
4. Whether or not the long-range IT plan is supporting the achievement of the organization's overall mission and goals?	1	2	3	4
5. Whether or not, prior to developing or changing the long-term Information Technology plan, the management of the information services function assessed the existing Information Systems, in terms of the degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses, in order to determine the degree to which the existing systems, support the organization's business requirements?	1	2	3	4
6. Whether or not the organizational model and changes made to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third-parties or the market, planning horizon, business process re-engineering, staffing, in or outsourcing, etc., are taken into account at the time of the planning process?	1	2	3	4
7. Is there any changed management procedure for making changes in the long-term plan?	1	2	3	4
8. Has the plan been communicated to the respective business owners?	1	2	3	4
9. Are there any existing change management procedures, for modification of the long-term IT plan?	1	2	3	4
10. Whether or not, the business strategy is documented and business objectives have been defined and the role of IT has been clearly spelt out in the business strategy?	1	2	3	4
11. Whether or not, Information Technology issues as well as opportunities have been adequately assessed and reflected in the organization's strategy and in its long and short-term plans.	1	2	3	4

(Contd)

12. Whether or not, assessments are made periodically by the bank to ensure that IT initiatives continue to support the organizational mission and goals?	1	2	3	4			
13. Whether or not, major developments in technology (hardware, software, communication, etc.) are assessed to know about their impact on the business strategy and for taking necessary corrective steps, wherever needed.	1	2	3	4			
14. Whether long-range IT plans are converted to short-range IT plans regularly for effective achievability?	1	2	3	4			
15. Whether or not the short-range IT plan covers the following: • Plan for initiatives specified in the long-range plan or initiatives that support the long-range plans • System-wise transition strategy • Responsibility and plan for achievement	1	2	3	4			
16. Whether adequate resources are allocated for achieving the short-range plans?	1	2	3	4			
17. Whether short-range plans are amended and changed periodically, as necessary, in response to changing business and Information Technology conditions?	1	2	3	4			
18. Whether assessments are made on a continuous basis regarding the implementation of short-range plans?	1	2	3	4			
19. Whether clear-cut responsibilities have been fixed for achieving the short range IT Plan?	1	2	3	4			
B. Organizing							
1 = Unclear, 2 = Somewhat unclear,							
3 = Fairly clear, 4 = Clear							
20. Whether a well-documented information security policy is available?	1	2	3	4			
21. Whether or not, this information security policy has been approved by the board of directors/ Top-level management?	1	2	3	4			
22. Whether or not, this policy has been communicated to the respective concerned audience.	1	2	3	4			
23. Whether or not the following major security areas are covered in the policy:	1	2	3	4			

(Contd)

160 *Information System Audit and Assurance*

• PC and LAN, MAN and WAN security • Physical security to IS establishments • Handling of confidential information • Handling of security incidents • Privacy related issues for outside entities • E-Mail security • Application security • Interface security • Password security • Operating system security, website security • Database security • Anti-virus and piracy policy • Archived and backedup data security • Vsecurity policy and consequence for willful violation of the security policy				
24. Whether a review process is in place for reviewing the policy at periodic intervals and/ or on any other occasion?	1	2	3	4
25. Do there exist lower level documented information security procedures which are derived from the top-level policies?	1	2	3	4
26. Is there any documented policy/procedure for recruitment of Information System personnel?	1	2	3	4
27. Is there any background check, conducted before recruitment?	1	2	3	4
28. Does the organization have a policy/procedure for entering into a confidential agreement with the prospective employee, for maintaining the confidentiality of the related organizational matter?	1	2	3	4
29. Does the organization have a policy/procedure for signing a conflict of interest agreement with the employee?	1	2	3	4
30. Does the organization have a policy/procedure for non-compete agreement?	1	2	3	4
31. Is there any process of providing orientation training to the personnel, recruited for Information System?	1	2	3	4
32. Is there a policy/procedure for training the personnel as per the job profile.	1	2	3	4
33. Is there sufficient cross-training or backup of identified key personnel to address unavailability?	1	2	3	4

(Contd)

34. Is there any structured, employee performance evaluation process, reinforced by an effective reward system?	1	2	3	4		
35. Are any appropriate and timely actions taken regarding job changes, job termination so that internal control and security are not impaired by such occurrences?	1	2	3	4		
36. Is there any practice of maintaining an employee handbook which contains:	1	2	3	4		
• Expectation of the organization						
• Abstract of the information security policy						
• Information about performance evaluation						
• Emergency procedures						
• Disciplinary actions against breach of policies and procedures						
37. Whether documented security policy is made available to all the levels of users, to the extent relevant to them?	1	2	3	4		
38. Whether continuous awareness programmes are conducted for security awareness?	1	2	3	4		
39. Whether the role of information security officer, with responsibilities for implementation of the security policy has been assigned?	1	2	3	4		
40. Whether detailed procedures for each policy statement have been developed?	1	2	3	4		
41. Whether suitable methodologies are adopted for implementation?	1	2	3	4		
42. Whether suitable security tools are selected for implementation?	1	2	3	4		
43. Whether the roles of those responsible for implementation are clearly defined?	1	2	3	4		
44. Whether the budgetary allocation for implementation of IS security is assessed and documented?	1	2	3	4		
45. Whether periodic security audits are carried out?	1	2	3	4		
46. Whether, on the basis of audit reports or any other vital information, suggestions for updating the security policies are conveyed to the right/appropriate level of management?	1	2	3	4		
47. Whether the management demonstrates adherence to the security policy?	1	2	3	4		

(Contd)

162 *Information System Audit and Assurance*

48. Whether new entrants are given adequate exposure to the security policy?	1	2	3	4			
49. Whether in case of breaches of security policy, the root cause is analysed and preventive and corrective actions taken?	1	2	3	4			
50. Whether incidence-reporting procedures have been followed?	1	2	3	4			
51. Whether the information security officer is made responsible for reporting non-compliance with approved policy and incidents of security breaches, to the top-level management, and for initiating and effecting corrective action?	1	2	3	4			
52. Has the organization gone in for strategic outsourcing for any Information System activity. (4 = Yes, 1 = No)	1			4			

If Yes, answer the following questions, from 53 to 59:

53. Is the process inherently dynamic?	1	2	3	4			
54. Is the process outsourced, standardized or stable?	1	2	3	4			
55. Does the organization have problems in acquiring skilled resources for that particular activity?	1	2	3	4			
56. Does the performance of this activity represent the core competency of the organization?	1	2	3	4			
57. Whether for the selection of an outsource vendor, the organization followed a structured process?	1	2	3	4			
58. Does Request For Proposal (RFP), for selection of an outsourcing vendor, have a right to the audit clause?	1	2	3	4			
59. Does the outsource partner have the business domain knowledge?	1	2	3	4			
60. Is there any conflict of interest in assigning the duties to the Information System personnel in the organization? (Please see the matrix given in the book)	1	2	3	4			

C. Leading

1 = Unclear, 2 = Somewhat unclear,
3 = Fairly clear, 4 = Clear

61. Is the management aware of the risks and controls in their Information System framework?	1	2	3	4			

(Contd)

62. What is the percentage of Information System personnel who left the organization during the last 1 year? (1: 0% to 20%, 2: 20% to 40%, 3: 40% to 60%, 4: 60% and above)	1	2	3	4			
63. What is the percentage of Information System personnel who were formally trained in new technology the during last 1 year? (1: 0% to 20%, 2: 20% to 40%, 3: 40% to 60%, 4: 60% and above)	1	2	3	4			
64. Is there any structured post training review process in the organization?	1	2	3	4			
65. Is the training given to the Information System personnel, commensurate with their present or future job profile?	1	2	3	4			
66. Is there any specific training given on information security to the Information System personnel?	1	2	3	4			
67. Do the in-house training institutions impart training on relevant areas of Information Technology?	1	2	3	4			
D. Controlling							
1 = Unclear, 2 = Somewhat unclear, 3 = Fairly clear, 4 = Clear							
68. Are there any regular reviews undertaken by the top-level management, regarding progress of the project undertaken?	1	2	3	4			
69. Is the organization following a balanced business scorecard method for exercising control over the Information Technology professionals?	1	2	3	4			
70. In the steering committee are the issues related to Information System security discussed? (4 = Yes, 1 = No)	1			4			
71. Whether disciplinary actions are taken on those breaching IS policy/procedures? (4 = Yes, 1 = No)	1			4			
72. Are most of the projects undertaken by the organization completed within the specified budget? (4 = Yes, 1 = No)	1			4			
73. Is there a documented procedure for obtaining financial sanction of IS projects/investment? (4 = Yes, 1 = No)	1			4			

(Contd)

164 *Information System Audit and Assurance*

74. What is the trend of the IS investment by the organization in the last 3 years? (If the variation is 0–20% then choose 1; 21–30%, choose 2; 31–40%, choose 3; greater than 41%, choose 4.)	1	2	3	4			

Score chart

S.No	Area	Performance		
		Poor	Adequate	Good
1	Planning	1–25	26–50	51 and above
2	Organizing	1–56	57–112	113 and above
3	Leading	1–9	10–18	19 and above
4	Monitoring	1–11	12–22	23 and above
Overall score		4–105	106–206	207 and above

Good

The management controls on the Information System function are satisfactory. The management considers Information System activities as part of their business functions and there is an effective strategic planning process in place. The users are aware of their roles and responsibilities. There are documented policies and procedures which are in accordance with global standards and these are practiced across the organization. The organization needs to sustain this, so that it can reap the benefits of competitive advantage.

Adequate

The management control on the Information System is in a stage of improvement. There seems to be a transition of the IT absorption process, in the organization from the consolidation to the controlled phase. The users are more or less aware of their roles and responsibilities. However, there should be an attempt to create greater awareness among the users. The policies and procedures are documented, as per the existing standards, but these need to be matured. Any laxity by the management at this stage, will be detrimental to the interests of the organization. More stress has to be given on the implementation of policies and procedures.

Poor

The management control on the Information System is not effective. There are no documented policies and procedures. Resources used for the Information

System function are not practical and realistic. The practices followed in the organization, as regards the Information System functions are not as per the accepted standards. The organization should give stress on setting up of an Information System framework and the initiative for this should come from the top-level management.

For an Information System auditor, auditing the management subsystem is not an easy task. Here, the auditor has to deal more with the management area than the technology area. The knowledge of organizational behavior is very important for the auditor at this stage. Nonetheless, the knowledge of IT will help the auditor in appreciating the role of the management. Another important point in the management control review is that at the end of the audit, the auditor has to comment on the effectiveness of the management control or in the other words comment on the functioning of the management, and you can now imagine, how difficult that is! You have to, after all, follow the code of professional ethics designed for Information System control professionals, recommended by various international organization like ISACA.

SUMMARY

In this chapter, we have learnt about the role of the management, from an Information System's point of view and the role of an auditor in reviewing the management subsystem. The management level role can be broadly classified into four categories, viz. planning, organizing, leading, and controlling.

In the planning stage, the management should define a strategic Information Technology plan, which should cover the basic questions of what, how, when, and why of the Information System. The long-range plan should also be converted to short-range operational plans at periodic intervals. The management should set up a framework which should *inter alia* help in framing, modifying, communicating, and implementing long and short-range plans. While discussing the setting up of an Information Technology framework, we also gave an example of a framework in a banking organization. Once the goals are earmarked in the strategic IT plan, the next step is gathering, allocating, and coordinating the resources needed to accomplish this goal. In this context, the organizing function of the management is very important. In the organizing function, we discussed policies and procedures, with examples from the banking sector. Apart from the Information Technology policy, we also discussed, the various human resources policies, relevant to the Information System. One of the very important organizing functions of the management is deciding about strategic outsourcing. Therefore, the why, what, and how of outsourcing was also discussed in details as, was the control requirement of outsourcing. Another

important area in the organizing function of the management is the setting up of the organization of Information System area. In this context, we have discussed various roles in the Information System functions, the possible conflict of roles, etc. We have also discussed, the possible organizational setup of the Information System area of a banking organization.

The leading and controlling functions of the management were discussed in a nutshell. In the controlling function, the basic requirement for the management is to give importance to controlling the output instead of the input. The controlling function of the management is broadly based on how to control finance and personnel. In this context, we have discussed, the balanced business scorecard method and in brief, the Critical Success Factor (CSF), Key Goal Indicator (KGI), and Key Performance Indicator (KPI). After discussing the role of the management, we also discussed the role of the auditor. At the end, a checklist was also provided to help the auditor formulate his/her opinion.

REVIEW QUESTIONS

1. What is management control on Information System? What are the broad areas which are typically management concerns? Describe what, a prudent management should perform in each area?
2. Why is planning important for the Information System? Discuss the role of the management in effective planning.
3. Give an outline for setting up of an Information Technology framework for a banking organization.
4. Discuss the role of an auditor in evaluating the planning process of Information System.
5. Briefly discuss each of the two types of major plans that must be formulated for the Information System function.
6. What are differences between policy, procedure, and standard? Describe with the help of examples.
7. Describe the control requirements for personnel recruitment and promotion in the Information System function.
8. Why is strategic outsourcing important from the control perspective? Discuss the advantages and disadvantages of outsourcing.
9. Give an outline of the selection and evaluation process of outsourcing partners for Information System functions/activities.
10. Discuss the organization of the Information System area with the help of examples.

MULTIPLE CHOICE QUESTIONS

1. Which one of the following functions in the information processing facility, if combined, can cause serious security concerns?
 - (a) Database administrator and system analyst
 - (b) Database administrator and application programmer
 - (c) System analyst and data entry
 - (d) System analyst and application programmer
2. Which of the following should not be included in an organization's IS security policy?
 - (a) Access authorization
 - (b) Access philosophy
 - (c) Importance of security awareness
 - (d) Identity of sensitive security features
3. Observing the personnel in the performance of their duties is a technique that an IS auditor might use while performing an audit. The technique will help him in identifying all the following, except:
 - (a) Security
 - (b) Awareness
 - (c) Organization IS policy
 - (d) Actual functions
4. When considering centralization versus decentralization of the Information System function, in which of the following are the three major dimensions of the decision, most likely be considered?
 - (a) Control, function, location
 - (b) Control, location, function
 - (c) Location, control, function
 - (d) Function, location, control
5. The risk associated with cross training is:
 - (a) Large turnover of staff
 - (b) Many people knowing the system
 - (c) Single person knowing all parts of the system
 - (d) Loss of financial resources
6. Planning in the Information System function is important because it:
 - (a) Determines the goals of the Information System
 - (b) Determines the means to achieve the goal

168 *Information System Audit and Assurance*

- (c) Coordinates the resources needed to achieve the goal
- (d) A and B
- 7. Non-compete agreement is used to prevent former employees from all of the following, except:
 - (a) Leaving, in the first place
 - (b) Defecting to a competitor
 - (c) Disclosing company's secrets
 - (d) Opening another business
- 8. Service level agreements establish:
 - (a) Minimum service levels to be rendered by IS management
 - (b) Minimum service levels to be achieved in the event of a disaster
 - (c) Maximum service levels to be rendered by IS support services
 - (d) Minimum levels of processing capabilities that can be affected by a disaster
- 9. Change management procedures are established by the IS management to:
 - (a) Control the movement of applications from the test environment to production environment
 - (b) Control the interruption of business operations caused by lack of attention paid to unresolved problems
 - (c) Ensure the uninterrupted operation of the business in the event of a disaster
 - (d) Verify that system changes are properly documented.
- 10. In a data center of a bank that has implemented centralized banking solution, the networking area can be combined with the following area:
 - (a) Security administration
 - (b) Computer operation/backup
 - (c) Help desk
 - (d) System administration

DISCUSSIONS AND RESEARCH QUESTIONS

1. What are the important points which should be considered while setting up an Information System management architecture? Discuss with the help of examples.
2. 'There are no technology solutions to management problems.' Discuss the statement in the context of the importance of management control in an Information System.

3. Implementation of policies are more important than framing them. Discuss.
4. Briefly discuss the difference between conflict of interest agreement and non-compete agreement. What precautions should be taken by the management in framing these?
5. Discuss the why, what, and how of outsourcing the Information System function, from the management's perspective.
6. Discuss the importance of balanced business scorecard in controlling the Information System functions by the management.

EXERCISES

1. Write a policy and related procedures on any area of the Information System function.
2. Draw an IT management framework for an E-Commerce organization.
3. Prepare a checklist for the management for selecting and evaluating the outsourcing partners.
4. What are the Information System roles, required for a data center of a bank, which is in a core banking environment. Describe the function of each role and their reporting structure.
5. Prepare the key goal indicators for the function. "Define strategic Information Technology plan".
6. Banking Technology institute is a large institute, with about 200 students and 2000 employees, offering a wide range of courses and services to the banking and financial sector. The existing computing facilities have been divided into two groups— an academic computing center, and a services computing center. Each group has its own hardware, software, personnel and so on and each operates independently from the other group, with an overall control that rests with the Director of the institute. The computing facilities at the academic center, take care of computing needs namely, payroll, students record, research, budgeting, financial planning, etc. whereas, the computing facilities at the service center take care of providing various services to the banking sector, charge back, and accounting of these services, etc.

Currently, the facilities of the service computing center are heavily over worked/used because of the variety of services offered to the entire banking and financial sector. A steering committee of the institute has been formed to examine the problem.

170 *Information System Audit and Assurance*

The steering committee had been given wide terms of references. In recent years, the institute found it increasingly difficult to find sources of private funding and to obtain government funds. The Director of the institute has asked the steering committee to consider the possibility of amalgamating, both the computing groups, selling the existing software and purchasing a large machine, that will serve both the centers. He feels that the centralizing computer facility could produce economies of scale. Because the academic computer will have substantial access capacity during the interim period, he also wonders if some service applications might be shifted to the academic computer.

Required: You are a member of the internal audit staff of the institute. The chair of the steering committee has asked the manager of the internal audit for his views on the proposed changes and he has asked you to brief him. Prepare a memo, outlining the advantages and disadvantages from the internal audit viewpoint.

5

Application Control Review

-
- ❖ Application system
 - ❖ Types of application system
 - ❖ Client server application
 - ❖ Web-based application
 - ❖ Importance of application system
 - ❖ Subsystem factoring
 - ❖ Boundary subsystem and controls
 - ❖ Input subsystem and controls
 - ❖ Data entry screen design
 - ❖ Processing subsystem and controls
 - ❖ Output subsystem and controls
 - ❖ Overall control
 - ❖ Application control and COBIT
 - ❖ Auditing application control
 - ❖ Testing application system
 - ❖ Testing application control
 - ❖ Conversion audit
 - ❖ Checklist for application control review
-

APPLICATION SYSTEM

Before discussing the application control framework, let us first see what an application system is? How is it important to the organization? What are the different types of application systems? After knowing this, we will proceed to learn how to ensure that the application systems safeguard assets, maintain

data integrity, fulfill the organizational goals effectively, and consume resources efficiently. In the end, we will learn about the role of an auditor in assuring the management about the efficacy of the application system. A sample checklist is provided at the end to help the auditor in forming his/her audit opinion.

THE APPLICATION SYSTEM

An application system is a set of interrelated components, designed for performing a particular business process or a group of business processes. All the activities of the business process can be carried out through the computer or the output from a computer system can be used intermittently as input for a manual system and then the output of the manual system can again be used as input for the computer system to get the final output. From an Information System Audit prospective, the entire lifecycle of the business process is important. Let us take an example of a business process in a bank, i.e. outward cheque clearing. This business process can be divided into the following activities:

1. Receipt of cheques and pay-in-slips (*challans*) from the customers and recording the data, related to both, cheques and pay-in-slips
2. Separate the cheques from the pay-in-slips and record the data for each, separately. The cheque total should tally with the total of the pay-in-slips
3. Sort out the cheques, bankwise and then take the bankwise total—this should tally with the cheque total described in 2 above
4. Encode the cheques with the help of an encoder, before presenting these to the clearing house. The total encoded amount should also tally with the amount of cheques in 2
5. Present the cheques in for clearing
6. On the second day, the bank will receive the cheques that have been returned, unpaid by the drawee banks
7. Mark the returned cheques, in the outward clearing register and then pass on the credit to the customer

From the above, you have seen that the process starts with receipt of cheques from the customer and ends with giving credit to the customer. In between, there are various activities, which may or may not be computerized. There may be an application software in the bank which takes care of a group of activities and receives input from a manual system and also provides output, which is used as input for a manual system. In fact, there are activities which

are controlled by a third party, i.e. clearing house, etc. From an auditor's perspective, the application system is a combination of a computer system and a related manual system.

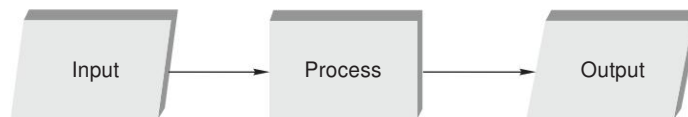


Fig. 5.1 Application system: Traditional way of thinking

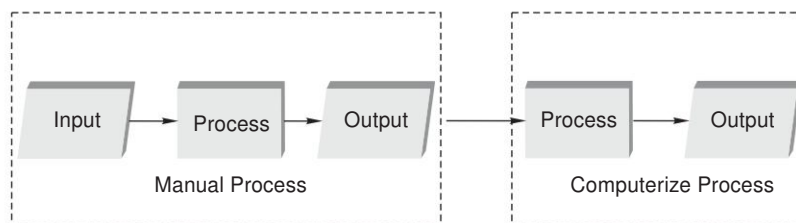


Fig. 5.2 Application system: The new way of thinking

TYPES OF APPLICATION SYSTEM

As regards the type of application software, its classification is context-dependant. Depending on use, application software can be divided into two, viz. single-user application and multi-user application.

Single-user Application

The application is basically designed for operating in a stand-alone environment which means that there is no file level or record level locking. Such kind of applications are mostly used for batch processing and are not used for Online Transaction Processing (OLTP). In case of banks, the Advanced Ledger Posting Machines (ALPMs) are examples of such kind of applications.

Multi-user Application

Using a single-user application in a network environment does not make it a multi-user application. 'Single-user' and 'multi-user' are all application level architecture. In case of a multi-user application, there is both file and record level locking and it is designed for working in a networking environment.

These kind of applications are used for online transaction processing. The Total Branch Automation (TBA) packages of a bank are examples of multi-user application.

Depending on the architecture, the application can be a client server application and web-based application. In fact, all web-based applications are also improvised client server applications, but all client server applications are not web-based applications.

Client Server Application

Client server applications work in a request–response way. A client is a piece of software which requests for some information and the server is another piece of software, which responds to that request. The client and server can reside in the same computer or in different computers. Between the client and server, there can be a number of tiers or intermediate computers like application server, database server, etc. Depending on the number of intermediate computers or servers between the client and the server, the architecture can be categorized as two-tier or three-tier or N-tier.

The transactions in a Automated Teller Machines (ATMs), are client/server applications. The client sends a request to the server, like a customer sends a request to an ATM. Just as the outcome of the ATM transaction depends on what type of information the customer gives the ATM when prompted, so does the outcome of a client's request for information from a server depend on the information given to the server.

The client sends a request to the server which is accompanied by the following information:

- Address for the server (Where do I ask for this information?)
- The request (What information do want?)
- The return address for the information (Where do I send the information?)

There must be a common protocol that both, the client and the server follow, to communicate with one another. On the Internet that protocol is TCP/IP. The server does most of the work in the relationship. It waits for requests, processes them, and then sends the client, the information requested.

Box 5.1**The ATM: A client/server application**

To understand the client/server relationship, consider something that most of us have become accustomed to: using the ATM.

Think of the ATM as the client. You utilize the ATM for various banking needs by entering your specific information request. Assume you need cash. You insert your card, from which your account number is read. When prompted, you enter your PIN (Personal Identification Number), how much money you want, and which account to access. The ATM then sends the request to a central server machine. The server machine processes the request, matches your PIN with your account, debits your balance, and sends the reply back to the client, the remote ATM site. The client then acknowledges the result of the request by sending cash and a receipt (you hope). Because all the clients share a common server, your account is always updated.

WEB-BASED APPLICATIONS—THIN CLIENTS

When we speak of a "thin" client, we are normally talking about a pure, browser-based solution, or a web-based application, where the server is the web server, residing in any web host (operating system) and the clients are the browsers. Depending on the application architecture, these can be of any tier. At the client level, there will be no software required by the user's PC, except for the web browser. A thin client should be completely browser-independent, and not require a specific vendor's browser or operating system. The advantages and disadvantages of the thin clients are as follows:

Advantages***No Download or Installation***

The most important advantage is the elimination of the need for any download and installation of user interface software on the user's PC.

***No Installation Conflicts,
Versioning, or Environment Issues***

Running the client user interface, directly from the browser, eliminates the potential problem of loading the client software in individual computers. When any new software is installed in a user's machine, any changes that the

installation program makes to the user's environment, may affect other, previously installed programs.

This can be particularly disturbing if it affects another vendor's software.

Available from Any PC with Browser

Thin clients can work on any system that supports a browser, opening up lesser-used operating systems such as Win 3.1, Macintosh, UNIX, etc. These would also be available on hand-held and Internet-enabled laptop machines. Being able to access information from any browser, also allows users to work from home or office, without having to carry configuration and other files between locations.

Instant Updates and Revisions

Thin clients allow instant distribution of updates and revisions from a central location.

Disadvantages

Low Level of Interactivity

Browser-based clients, due to the inherent limitations of the medium, are more static and "flat" than program-based "thick" clients. Since the browser is a somewhat prettier version of the "dumb terminal" and all interaction, requiring user input is forms-based, there is a lower level of interaction between the user and the thin client. For example, it is difficult to change screen entries based on previous entries, i.e. changing the items in a subgroup list, depending on the previous choice in a group list. Some of this type of interactivity is possible through scripting on the browser page, but as of now, it is highly vendor-dependent.

Navigation of Multiple-browser Screens to Emulate Current Client Screens

Due to the low level of interactivity, some actions that are presented entirely on one screen, in the thick client, may now span multiple screens. Since each screen presentation involves a round trip to the web server, this process will be somewhat slower than the single screen approach. This can be minimized with some re-designing of the user interface workflow, but by and large, thin clients require more "clicks" than thick clients.

Must Write to Lowest Common Browser

Due to the ongoing "browser wars" and rapidly changing technology among various browser vendors, it is currently difficult to take advantage of the newest and most exciting features of the latest browsers. All thin client user interface software must be written to account for the older, lowest common denominator browsers, thereby, slowing down the introduction of newer or enhanced browser functionality.

Limited Access to Services on User's Machine

The browser sets up its own "sandbox" environment for the thin client, limiting its access to services on the user's PC. For example, printing from the thin client is currently limited to a print of the browser window and elaborate formatting is not available. In addition, the thin client has limited access to disk storage on the user machine thereby, forcing storage of preferences, parameters, data files, etc. on the server.

THICK CLIENTS

The "thick" client is a system that is designed to have software loaded on the user's PC, whether by floppy, CD, or over the net. It is usually represented as a windowed application.

Advantages***Rich Screen Functionality, High Level of Interactivity***

Since the client is a program installed on the PC, it can be made to perform virtually any function, desired. This allows screen choices to affect other parts of the screen or application, etc. The application appears more interactive and "live" to the user. It also appears to be faster, since the client's machine is performing some of the processing and fewer trips are usually made to the server.

Required Client Adds Security, Persons without Client cannot Access System

Having a client application, increases security to a certain extent, as outsiders without the application installed on their PC will not be able to easily access server side information.

No “Sandbox”, Client is Able to Access Printer, Disk

As outlined above, application-based clients have more access to the client's PC utilities, allowing more elaborate print functionality, storage access, multimedia display, etc.

Disadvantages

Updates, New Features, and Bug Fixes, Require Users to Download and Install Client Side Software

As discussed above, every user interface change, requires client software redistribution to the PC. This is the biggest disadvantage of a thick client. Even when extreme care is taken in constructing installation scripts, the variation in users' machines is great enough to cause problems in some percentage of cases. These cases require help desk intervention and sometimes even a site visit to be corrected. Under the thick client model, new features, bug fixes, and other updates that require user interface changes, cannot be implemented in production until the new client user interface is built, distributed and installed among the user community.

Server Must Account for Multiple Versions of Clients and Increasing Complexity

Versioning is often an overlooked thick client issue. Since users rarely change over to new client software applications, all at once, and some stay with the old client forever, the server side must recognize and continue to accept requests from old or obsolete client software. This, dramatically increases the complexity in both, design and test of future server architectures, since they must account for these past client formats.

Inability to Access System from “Ad hoc” Locations Unless Client Installed.

If the client software is not installed on the user's machine, information cannot be accessed from the server. This can be a problem for users working from home or multiple-work locations. It also means they cannot, on demand, get an answer to a spontaneous request, as they could, if they could, access server information from any browser-enabled machine.

THE IMPORTANCE OF THE APPLICATION SYSTEM

The application system assumes importance on the basis of the business processes it carries out. The importance of the application system is directly proportional to the importance of the related business processes for the organization. For example, in the case of a bank, an online core banking application will be more important for the organization than an Advanced Ledger Posting Machine (ALPM) application. Similarly, an ERP application, for any organization, will be more important than all other applications.

APPLICATION CONTROL

Whatever be the type of application system, the basics of control in all the systems, remain the same, although, the implementation of these, differ from application to application. In this chapter, we will discuss the generic controls in the application system.

For convenience, we will first factor the application system into various subsystems, depending on their functionalities and then, discuss the components of each subsystem and the control requirement for each of these, separately.

SUBSYSTEM FACTORING OF THE APPLICATION SYSTEM

Typically, an application system accepts data through various input devices, processes these data as per the business logic and then gives the necessary output. So, considering the functionality, we can factor the system into six subsystems, viz.

- Boundary control
- Input control
- Processing control
- Database management system control
- Output control
- Overall control

This entire factoring is based on a typical functioning of the application software. For accessing the application, there is always a boundary which can be implemented by different kinds of access control mechanism and also by various cryptographic controls. Once the boundary is successfully crossed,

the user will have the necessary interfaces for entering data. These interfaces can be screens, menus or even the command prompt for giving input to the application system. In fact, these inputs can enter into the processing system through any communication system and finally, the output is delivered to the user. During all these stages, we need to have appropriate controls to ensure that the entire application system safeguards assets, maintains data integrity, fulfills the organizational goal effectively, and consumes resources efficiently. The lifecycle of the entire application system control is depicted in Fig. 5.3.

In the following section, we will discuss each stage of the application and the relevant controls associated with it. After discussing the generic controls required for each subsystem, we will discuss the audit trail and existence control, under each subsystem.

Boundary Subsystem and Controls

The basic objectives of the boundary subsystem is to ensure that:

- The system has an authentic user
- The user gets authentic resources
- Users are allowed to employ resources only in restricted ways

Now, the most important question is how to achieve these objectives. This basic problem in achieving these objectives is the common knowledge base of the user and the system, which is needed for validating or authenticating each other. Any compromise in the knowledge base, either by the user or by the system or by a third party, without the knowledge of either the system or the user, poses a great challenge to the implementation of the boundary control.

Access Control

Each and every application system should have an initial boundary and access to the system should be restricted as per the business policy. The various kinds of access control procedures that are widely accepted in the industry are as follows:

Logon IDs and Passwords

This is one of the most common type of access control procedures, where there should be different levels of users for the application system and access is allowed after producing the user ID and password, which is unique for each user. Some of the important control requirements for such systems are:

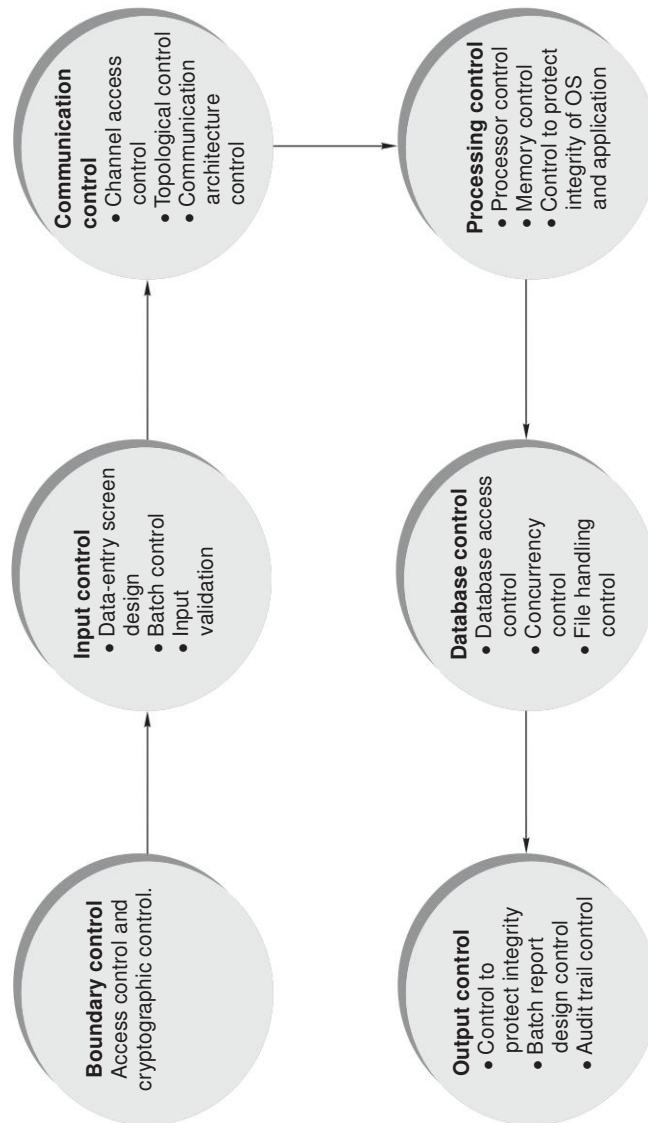


Fig. 5.3 Lifecycle of the application

- The user ID and password should change frequently as per the password policy of the organization
- The minimum length, combination of characters in the password (alphanumeric), should be part of the password policy
- The user ID and password are stored in a backend database, with proper access control
- The password should preferably not be stored or travel in a network in a clear text, without proper encryption
- The system should only prompt the user about the genuineness of the pair (user ID + password), not of one alone

Interrogation System

There can be some additional queries after user ID and password validation, like "mother's maiden name or passport number or any other identity which will further establish the authenticity of the user.

Smart Card

Smart cards date back to 1974 when the Frenchman, Roland Moreno, was granted a patent on the concept of the smart card. The patent applications mention, portable and protected data storage and take no stand on the implementation methods of the smart card.

What is a Smart Card?

A smart card is a microchip-equipped, payment card. It can be a bank and/or credit card, SIM card for a mobile phone, electronic ID card or a combination of these cards.

A smart card is the size of a credit card or a smaller SIM card and is equipped with an embedded microcircuit which contains memory and a microprocessor, together with an operating system for memory control. The smart card is a secure storage location for secret information.

One card can be used for many different applications without mutual interference. The card can store data such as personal information, money, or other information whose alteration or disclosure might be risky. The card may also store encryption keys, which the card user can use for tasks such as key exchange, network identification, or digital signature.

The smart card can also be used for decoding encrypted messages and for digital signatures. The card makes it possible to avoid reading the key into the computer for software encryption, which means that the risk of disclosure is reduced considerably.

The smart card despite a similarity in appearance, is not the same as the so-called memory card which is suitable for disposable data storage. Memory cards are, in general, used as phone cards or other disposable means of payment.

A drawback to memory cards is their weak security. Unlike smart cards, they have no operating system that controls memory use, and their use may be subject to the use of a card PIN. However, the security of the memory card is not as strong and versatile as that of the smart card.

Smart Card Operating System

The functional characteristics of the smart card are determined by its operating system. The operating system differs from traditional operating systems, in that, it is the only program, run by the card processor. The directories and files on the card may be assigned operating conditions. The operating system receives outside commands and executes them, provided that certain processing conditions are met. The processing conditions may include the requirement to enter the user's PIN or a strong authentication of the reader. The operating system is also responsible for the control of the RAM and the EEPROM.

Operating systems used in smart cards resemble disk operating systems used in PCs. Operating systems provide a hierarchical tree structure and very versatile options for specifying access rights. For this reason, a directory designed for smart cards, together with its files and access rights is called an application.

Smart Card Features

The smart card is

- Personal
- Portable
- A security token

The Smart Card is Used for:

- Electronic identification
- Electronic signature
- Encryption

KEYSTROKE DYNAMICS

Keystroke dynamics, also called typing rhythms, is one of the most eagerly awaited of all biometric technologies in the computer security arena. As the name implies, this method analyzes the way a user types at a terminal, by monitoring the keyboard input a thousand times per second. This can be

compared to the days of the telegraph, when operators would identify each other by recognizing "the fist of the sender." The modern system has some similarities, most notably that the user does not realize he/she is being studied, unless told. Also, the better the user is at typing, the easier it is to make the identification. Both, the National Science Foundation and National Institute of Standards and Technology, USA, have conducted studies, establishing that typing patterns of individuals are quite unique.

The advantages of keystroke dynamics in the computer environment are obvious. Neither enrollment nor verification detract from the regular workflow, because the user would be making keystrokes anyway. Since the input device is the existing keyboard, the technology, costs less. Keystroke dynamics can also come in the form of a plug-in board, built-in hardware and firmware or software. Still, technical difficulties abound in making the technology work as desired, and half a dozen efforts at commercial technology, have failed. Differences in keyboards, even of the same brand and communications protocol structures, are challenging hurdles for developers.

BIOMETRIC SYSTEM

Biometric technologies are defined as "*automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic.*" Let's extract the key words from this definition and examine each.

Automated Methods

The term biometric device in the access control industry implies that three major components are present in it:

1. A mechanism to scan and capture a digital or analog image of a living, personal characteristic
2. Compression, processing and comparison of the image
3. Interface with application systems

These pieces can be configured in a variety of ways for different situations. A common issue is where the stored images (reference templates) reside: in a card, in the device or in a host. The word "automated" is necessary for our definition because without it, we would also describe a variety of very common, but significantly less reliable, identification techniques such as a photo or inked fingerprint on an ID badge.

Identification and Authentication

This is arguably the most important aspect of biometrics, because the products associated with each category are vastly different. *Identification*: Identification occurs when an individual's characteristics are being selected from a group of stored images. Called a "one-to-many" search, the question put to the machine is "Do I know you?". The search algorithm will search a database and return a likely list of candidates in a matter of minutes. *Authentication*: Authentication occurs when an individual makes a claim of identity by presenting a code or a card. Called a "one-to-one" search, the question put to the machine is "Are you who you claim to be?" In this sense, the individual's characteristics are being measured against an existing image that is stored on a token or in a local database with the image presented.

Living Person

While this may seem like an obvious requisite, it is nonetheless, important to the definition. One of the first questions newcomers in the field ask is, "What about a latex finger, digital audio tape, plaster hand, prosthetic eye, etc." The answer is that many, but not all devices include methods of determining whether or not a 'live' characteristic is being presented. The methods are sometimes ingenious and usually simpler than would be expected. The term "living" also separates the biometric industry from the forensic identification field, although basic principles transcend the boundaries of both areas.

Physiological and Behavioral Characteristics

The final point in the definition is the difference between physiological and behavioral characteristics. A physiological characteristic is a relatively stable physical characteristic, such as a fingerprint, hand silhouette, iris pattern, or blood vessel pattern on the back of the eye. Such characteristics are basically unchanging and unalterable without significant threats. A behavioral characteristic is more a reflection of an individual's psychological makeup, although general physical traits, such as size and sex, have a major influence on them. The signature is the most common behavioral trait used for authentication. Other kinds of behavior that can be used, are how one types at a keyboard and how one speaks. Because of the variability, over time, of most behavioral characteristics, many of these machines update their enrolled biometric reference template each time they are used. After many successful accesses, the template may become significantly different from the original

data. The machine would also have become more proficient at identifying you. Generally, behavioral biometrics work best with regular use.

The differences between physiological and behavioral methods are important for several reasons. First, the degree of intrapersonal variation in a physical characteristic is smaller than in a behavioral characteristic. For example, except in the case of an injury to the finger, your fingerprint remains the same, day-in and day-out. A signature, however, is influenced by both, controllable actions and less controllable, psychological factors. Developers of behavior-based systems, therefore, have a tougher job, adjusting for intrapersonal variation. For example, it is easier to build a machine that guides you to place your hand in the same position, every time than it is to build algorithms that take into account emotional states or a person's sniffles. The downside of machines which measure physical characteristics is that they tend to be larger expensive and may be seen as threatening to users. Behavior-based biometrics however, often score better on these counts. Both techniques provide a significantly higher level of identification and accountability than passwords or cards alone. Because of these differences, no one biometric can serve all the needs. A company may even decide to use different techniques in different parts of the same access control system. For example, voice verification may be used for executive suites, and fingerprints may be used for computer rooms.

TERMINAL RESTRICTION

In such kind of access control, the access to the application is restricted to the designated terminal so that only the required and authorized persons can access the application. In case of a local area network, the terminal restriction is carried out through the network operating system.

TEMPORAL RESTRICTION

In case of temporal restriction, the access to the application is restricted on the basis of time. Let us say, for example, an application for cash payment of a bank can work only during the customer hours. This is an example of temporal restriction.

USAGE CONTROL

Application usage control deals with the giving of controlled access to the application. After a user is given access to an application, it should be ensured that the user gets access to the menu on a "need to know" basis. This is about

giving restricted access of the application to the user, based on the profile of the user, with respect to the application. There are three main controls that need to be noted while accomplishing usage control. The relevance of the following controls may differ from application to application, depending on the nature of the technology used in the application.

Navigation Control

Navigation control in an application, ensures that the user carries out the activities, he/she is authorized to perform and only relevant information is displayed to the user. Such control can be exercised by first, identifying the user and then allocating the resources accordingly. The resource allocation is done by manipulating the user interface, programmatically. Either the user, depending on the role profile, is given a fully customized interface or the same interface is given to all the users. While customizing the navigation, controls the flow, the tab stops at the relevant fields, depending on the role profile of the users.

The following figure depicts the area of function of the navigation control. Let us take a library application as an example. There are two types of profiles in this library application.

- Librarian
- Member

There may be many operations in the library applications like entering details of new books, issuing books, browsing through available books, application for reserving a book, etc. Based on the profile of the user, they have access to the operations. The "Librarian" profile user has the right to enter new entries of books, issue books, etc. These are some of the menu options in the menu that appears on the screen when the user with the profile of librarian, logs into the application.

The "member" profile on the other hand can only view the books in the library and apply for the issue of a book. Thus, only these two options should appear on the screen when a user with the "member" profile logs into the library application. This example is depicted in Fig. 5.4.

Direct Entry Control

From a user's perspective, it is the application, which matters, not the other utilities, available in the computer. From the control angle, the user should have direct access to the application without exposing him/her to the operating

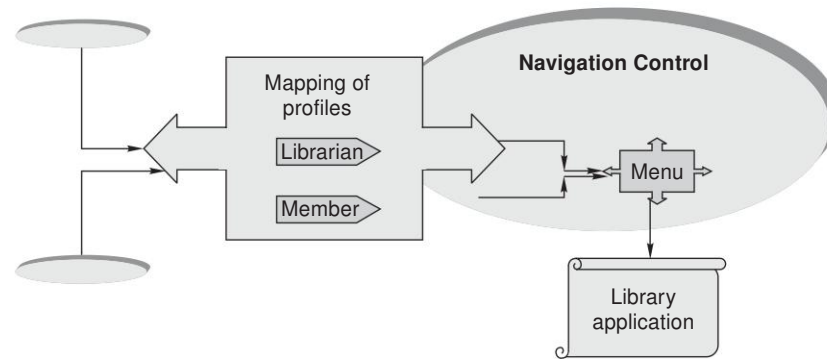


Fig. 5.4 Navigation control

system. This kind of direct entry control can be achieved by the following ways:

- **Set up in the boot configuration file:** A boot configuration file is a file that gets executed when a user logs into the operating system. This file contains a set of instructions that get executed one by one. In the Disk Operating System (DOS), such type of functionality is achieved by the Autoexec.Bat file. This is a batch file that has many DOS commands in it. A command to execute an application can be given in this file. So when the system boots, the commands in this file are executed and the user is directly taken to the application, instead of the command prompt
- **Login scripts:** In many operating systems, mainly the network operating systems, like Novell network, windows 2000, etc. the same thing can be achieved by appropriately modifying the login script. A login script is a set of instructions that are executed automatically when a user logs into a server. They are essentially batch files, which are used for many purposes, viz. creating user or group home directories, creating network drive mappings, and ensuring that certain programs (such as virus scanners) are run. In addition to these, login scripts can be written for specific users for taking them to specific applications directly, as per their role profile, without exposing the command line interface of the operating system to the users

Following are the important points, which should be taken care of while implementing direct entry control:

- It should be necessarily ensured that an exit from the application should log out the user from the operating system

- The scripts that are run are usually batch files, which are a set of commands. These commands can be stopped by a combination of keystrokes. For example, any DOS commands, during execution can be abruptly ended by pressing the Ctrl and break keys. So if the script is running and Ctrl and break are pressed, the script will stop running and the user will have access to the command line interface of the operating system. Therefore, while running the login script, the break option should be disabled

Concurrency Control

Concurrency control deals with the issues involved in allowing multiple people, simultaneous access to shared entities, whether objects, data records, or some other representation. To understand how to implement concurrency control within your system, you must start by understanding the basics of collisions—you can either avoid them or detect and then resolve them. The next step is to understand transactions, which are collections of actions that potentially modify two or more entities. An example of a transaction is, a transfer of funds between two bank accounts. The transaction consists of debiting the source account, crediting the target account, and recording the fact that this occurred. In the case of applications, written in high level languages like COBOL, etc. which use file systems at the back end instead of database management system, the concurrency control is implemented by writing program codes. In the case of database management systems however, the concurrency control is built into the system. Therefore, there is not much need to enforce this by writing software codes.

AUDIT TRAIL CONTROL OF THE BOUNDARY SUBSYSTEM

Audit trails are basically the primary source for building the profile of past behavior of any system/subsystem. Broadly, audit trails can be classified into two categories, viz. operational audit trail and accounting audit trail.

Operational Audit Trail

Maintains a record of resource consumption, associated with each event of the system/subsystem while, the *accounting audit trail* maintains the record of each event within the system/subsystem.

Accounting Audit Trail of the Boundary Subsystem

Audit trails are very good friends of the auditors. From a control perspective, it is not the presence or absence of the audit trails which matters. What really matters is the content of the audit trail and the control over the audit trail itself, so that the auditors will be able to effectively assess and evaluate the profile of the past behavior of the system/subsystem. In the case of boundary subsystem, the accounting audit trail contains:

- Identity of the user-to-be of the system
- Authentication of the information supplied
- Resource requested
- Action privileges requested
- Terminal identifier
- Start and finish time
- Number of login attempts
- Resource provided/ denied
- Action privileges allowed/ denied

This data will allow the auditor or sometimes even the management to recreate the time series of the events that occur when a user attempts to pass the boundary control. The analysis of the audit trail can either be done manually or by using various customized audit tools.

OPERATIONAL AUDIT TRAIL OF THE BOUNDARY SUBSYSTEM

It may be seen that the data collected in the accounting audit trail would also help the auditor to assess the resource utilization in the boundary control. For example, recording the start and finish time and the resources requested, will facilitate an analysis of resource usage within the subsystem.

EXISTENCE CONTROL OF THE BOUNDARY SUBSYSTEM

Existence control is basically the contingency requirement of the system/subsystem. Imagine that the boundary subsystem fails (not compromised). Then there are two things which can happen, i.e. either nobody will be allowed or everybody will be allowed. While allowing everybody is a dangerous proposition, not allowing anybody will also restrict genuine users. So the

existence control in the boundary subsystem should be designed after taking these basic things into consideration.

In the case of a boundary subsystem, the existence controls are simpler than those in other subsystem. If failure occurs, the controls, usually, do not attempt to restore processing to the point of failure. Instead, users must commence the sign-on process, afresh. For example, in case the user gives either an incorrect user ID or incorrect password, the boundary control will fail. The control however, should be designed in such a manner that in either case the user is prompted to submit the pair (user ID and password), instead of just the one which is entered incorrectly. This requirement also provides protection against the situation in which the original user has left the terminal device and has been replaced by another user.

INPUT SUBSYSTEM

Once the user has got access to the application, the first task is usually, entering data. The data can be entered manually, through the keyboard, through a custom-designed data entry screen, or direct reading through Optical Character Recognition (OCR), Magnetic Ink Character Recognition (MICR), image reader, Point Of Sale device (POS), and Automated Teller Machine (ATM), etc. or through direct entry through a personal computer, touch screen, mouse, joystick, trackball, voice video, and sound, etc.

Whatever may be the input device, the input control procedures must ensure the following things:

- Every transaction to be processed is received, processed and recorded accurately and completely
- Only valid and authorized information is entered
- Transactions are processed only once
- In an integrated system environment, since the output generated by one system is the input for another system, the edit checks, validations, and access controls of the system generating the output must be reviewed as input/originating control

Validation of Input

Input validation is one of the fundamental aspects of application control. In fact, most of the problems in the application can be prevented if there are proper validation controls in the applications. The input controls can be at different levels, viz. field level, record level, batch level, and file level. Some of the important controls, at various levels are discussed in the following sections.

FIELD LEVEL INPUT CONTROL

Sequence Check

In such kind of checks, the application, prevents any entry, which does not follow a particular sequence. Let us take the example of cheque payment in a bank, where the system should prevent entry of any data where the cheque number is not within a range supplied to the customer and also not in proper sequence. Another example could be that of invoices, which are numbered sequentially. Let us assume that the day's invoice begins with 1001 and ends with 2000. If any invoice, numbered beyond 2000 is encountered during processing, that invoice will be rejected by the input subsystem.

This sequence check should be implemented by taking the input string to the backend database and then validating. Control of the backend database is very important for the sequence check to be effective.

Limit Check

In such kind of validation, the check should ensure that the data does not exceed a particular limit. For example, the basic pay of a person should not be more than some particular amount. Although, it will always be better to implement such control by writing a few lines of script in the program code, from a control perspective, it is always better to parameterize it by keeping it in any database at the backend.

Range Check

The range check is slightly different from the sequence check, in the sense that in the case of range check, the data should be within a predetermined range of values. For example, the product type code may range from 200 to 500. Any code outside this range should be rejected by the system. The codes may not be in sequence as in the case of sequence check.

Set Mapping

Set mapping ensures that the input data is validated against a predefined set of values. This is also a sort of validity check where data validity is in accordance with certain predetermined criteria. For example, a payroll record contains a field for marital status and the acceptable status code is either M (Male) or

F (Female). If any other code is entered, it should be rejected at the input stage itself.

Master Reference

In the case of master reference, the input is validated as per the master database. For example, in the case of entering the bank name on cheques that have to be sent for clearing, the name and code number of the bank should be validated by a master database. In fact, as per prudent practices, the users should not enter such data, but should pick up the required data from a drop down list of banks, which are therein the master database.

In the case of a master reference, the points related to control, which the auditor should look at are:

- In the input form, whether the master reference data are entered or picked up from a drop down list.
- If it is from a drop down list, then whether it is hard coded or taken from a database. In case it is hard coded then it cannot be called it a true master reference. Such applications are not scalable, which means that for any change in the master or reference data, there will be a need for change in the program.
- In case the reference is from a backend database, the control concerns are 'who populates the table?' 'Is there any proper change management procedure for this?', etc.

Imagine the case of a stop payment instruction, given for a cheque/ instrument. Now the input form for passing the cheques, has got the utility for validating the cheque number, cheque date, bank name, etc. from the stop payment database at the backend. But the data input clerk who enters data for passing the cheques has also got complete access to the stop payment, database through a user interface. Is this right?

Size Cheque

In such kind of controls, it is ensured that data cannot be entered beyond the field size, set by the program. Take the example of the age of a human being. The age field in this case should not accommodate numbers of four digits i.e. "9999". Such kind of controls helps in restricting human errors by the data entry operator and at the same time give some kind of lower level validation to the data.

RECORD LEVEL INPUT CONTROL

Reasonableness

In case of the reasonableness control, it is ensured that the data, in combination with other fields are reasonable as per the standards set by an organization. Take the example of a control that an organization needs to adhere to, i.e. the salary of a low designation employee cannot be higher than that of a high designation employee. Also, take the example of a control that requires that the hike in salary of an employee cannot be more than 50% in any particular month. Such controls are basically higher level controls which are used by the management to check the reasonableness of the output.

Valid Signs—Numeric

In such kind of a control, it is ensured that the correct sign is used in the record. For example, there can be a control to ensure that none of the fields in the record are less than zero.

Size of the Record

Such controls are necessary for records with a variable field size. The maximum size of the record can be fixed by such control. Let us take the example of a buffet lunch. Here, you are allowed to consume any item, for any amount, but your total bill is fixed and does not exceed a certain amount. In such cases the ceiling is fixed by the control.

Sequence Check

In such kind of controls, it is ensured that in case of logical records, spanning more than one physical record, the sequence number is correctly stored. For example, multiple screens might be required to enter all the data about an event, and the data from each screen might be stored as a physical record. The input program might check the sequence of the physical records it receives.

BATCH LEVEL INPUT CONTROL

Although batch control has lost its relevance, as most of the computing is done on the basis of On-Line Transaction Processing (OLTP), still some of the basic controls necessary for batch input, both for physical batch and logical batch are as follows.

Control Totals

Before describing about control totals, let us describe in brief, the various types of batches. In case of *physical batches*, source documents are received and then consolidated into one batch. After consolidation and necessary controls, the batch is submitted to the computer. In the case of *logical batch*, several data entry operators enter the transactions and finally it is logically consolidated into batches and then submitted to the computer.

Since in each case, there is consolidation before submission, there should be some control to ensure that the sum of the individual totals should equal the batch total. These totals can be those of any fields or a combination of fields, which can be chosen for such purposes. Let us take the example of encoding of checks before submission to a clearing house or a cheque processing center. In case of encoding, the amount, transaction number, and endorsement are encoded on the cheques/ instruments. After encoding a certain number of cheques, say 200, a batch ticket is generated, on which is printed, the total amount encoded, for the two hundred instruments. After some batches, before submission to a cheque processing center, a block ticket, which is a sort of control total, is generated. The sum of the amounts of the batch tickets should tally with the control totals mentioned on the block ticket.

Transaction Types

Some additional controls in the batch inputs could be the transaction types. This kind of control ensures that all the input records in the batch are of the required transaction types. Let us take the example of a batch input of loan disbursements. In such cases, the transaction type control will ensure that all the transactions are of a debit nature.

Batch Serial Number

This is again, another type of batch control, where each input record in the batch is given a unique serial number that has been assigned to the batch.

Hash Total

In such kind of controls, it is ensured that a predetermined numeric field, existing for all documents in a batch, agrees with the total number of documents processed. For example, the source document serial numbers can be totaled and used as a hash. Let us take the example of the Inter Branch Reconciliation (IBR) application of most of the banks. In these cases, the inter branch

transaction data is obtained from the centralized banking application and uploaded into IBR application in a batch. To ensure the integrity of individual transactions, a hash is obtained from some of the key fields of each record, i.e. issuing branch code, responding branch code, inter branch advice number (system generated), transaction type, and the amount. The entire file, containing the records and the hash is encrypted with a symmetric key and the key is distributed across the branches to decrypt the file.

File Level Input Control

Sometimes, inputs are taken from certain files which may not be part of the same application system or even if they are, the files are used by other applications as well. In such cases, it is very important to ensure at the time of input that the data is obtained from the correct file. Such controls can be ensured by the following means.

Internal Level

The input validation program, checks to ensure that it is assessing the file with the correct name. This type of control is required for applications, developed using high level languages like COBOL, which uses ASCII file at the back end for storing and retrieving data.

Generation Number

This is another layer of control, which is meant for ensuring that the correct version/generation number of the file is used for the input.

Retention Date

In this case, the input validation program, checks to ensure that it is not using a file whose retention date has expired.

Control Totals

Control total is again, a kind of hash, which is calculated by taking different parameters from the file. The input program should be designed to generate the hash, compare it with the original hash, and take a decision about whether the file should be accepted for processing or not.

Box 5.2**Three important tips for auditors for input control**

1. *The likelihood of error in the data input is directly proportional to the amount of human intervention in the input process.*
2. *As the time interval between detecting the existence of a state or event, and input of the state or event to an application system increases, the likelihood of occurrence of errors also increases.*
3. *Use of special input devices or input subsystem within an input system, increases the reliability of the input data.*

Since most of the input controls can be put in place, at the data entry screen level, it would be useful, if at this stage, we discuss some of the control issues on designing a data entry screen.

DATA-ENTRY SCREEN DESIGN

A properly designed data entry screen, reduces the likelihood of input errors. Some of the best practices in the data entry screen design are as follows.

Screen Organization

- Screen should be uncluttered and symmetrically balanced
- All the information, needed to perform the task must be on the screen or if there is any requirement of multiple screens, there should be a logical break between the screens
- There should be spaces on the screen for displaying various messages like 'help', 'error', etc.
- The screen organization should be consistent across the organization

Some of the well-designed screens are depicted in Fig. 5.5.

The Screen Caption

- The caption of the data entry screen should be context-specific. For example, for data entry of a new employee, the caption should read something like "add new employee" instead of simply saying "Data entry screen"

- The caption of the screen or the data entry form should not be allowed to blink as this creates unnecessary distraction
- The caption should be in bold and in a font size slightly bigger than the other items on the data entry screen

M. John Kingsly
Research Associate

IDGSTNET V2.0
An EAI solution of IDBT

Leave Menu
Leave Card
Apply
Apply Half Day CL
Cancel
View Status
Help Desk
View Holidays in this year
Help
Home

Name: M. John Kingsly
Designation: Research Associate
Application Date: 12/10/2003
Id: RES48
Reporting to: D P Dube

Type of Leave: ☐ CL
From:
To:
Purpose:

Submit

(Screen with help and list box)

IDGSTNET V2.0
An EAI solution of IDBT

Add Long Term Contract Staff

Name:
Role: Director
Joining Date:
Valid till Date:
Designation:
Work Area: Projects
Status: User
On Deputation: ☐ Yes ☒ No

Reporting To: A Deepthi
Project: A Keshava Rao
Gender: ☒ Male ☐ Female
Date of Birth:
Address:
Telephone:
Email:

Submit

Fig. 5.5 A well-organized screen with radio button, check box, and list boxes

Field Design

- The data entry fields should immediately follow their respective captions, either in the same line or just below the captions

- Sometimes, the field itself should have some caption or help tabs that appear on the screen, by simply pointing the mouse to the requisite field. For example, in a Total Branch Automation (TBA) application, at the close of the day, the closing cash balance has to be entered by the user in the form of a negative figure. In such cases, it will be a good idea for the field titled, "closing cash balance", to have a sub-caption like "enter the amount in minus". This can also be achieved by doing some field level validation
- In case of direct data entry, let us suppose that there is an option for confirmation, i.e. "Yes" or "No". In such cases, the default option should always be "No". Otherwise the likelihood of wrong data input, increases

Tabbing and Skipping

- Automatic skipping to a new field should be avoided, as it can lead to field-size error
- Tabbing should be made mandatory for skipping to the next field, it may require an additional keystroke, but the operator's typing rhythm is maintained

Color

- Color should be used sparingly and consistently
- Only a few colors that are widely spread along the visual spectrum like red, yellow, green, and blue (RYGB), should be used
- Color should be consistent across activities. For example, for data entry there should be one color; for edit, another color; for alert, a different color, etc. Such kind of practices also reduce the programming effort
- Some colors are normally associated with certain activities. Therefore, it is prudent to use only those colors, so that it becomes easier for the users to the meaning of the colors. For example, error messages are normally associated with the color red
- Accommodate users who are color blind by using other means, viz. uppercase and lowercase texts, to differentiate captions from the data, entered by the users

Prompting and Help Facility

- Help should be context-specific and granular or minutely detailed
- There should be a space on the screen to display the help section
- Common and general help should be accessible by the use of a common function key, i.e. F1
- Hyperlinks should be provided in the help section to take the user to related topics

The screenshot shows a 'CheckOut Details' form with the following fields: Program Name (Rashmi Test), Participant Name (Muskaan), Guest Speaker (Other Occupant (---Check In Date)), CheckInTime (1:31:00 PM), Allotted Room No (103), CheckInDate (Nov 12 2003), and Block Name (Block A). A pop-up window titled 'Microsoft Internet Explorer' displays a warning icon and the message: '- Kindly enter the Received Amount , if "Nil" enter 0'. Below the form, a summary table shows: Room Rent perday Rs. 1000, Days accounted for 29 Days, Room rent amounts Rs. 29000, Service Bill amounts Rs. 39, and Total Bill in Rs. 29039. A 'Recieved Amount in Rs.' field is empty, and a message states 'Participant will be Checked out at 12/11/2003, 10:51 AM'. A 'Check Out' button is at the bottom.

Service Name	Quantity	Rate per unit in Rs.	Amount in Rs.
News Paper	1	8	8
News Paper	2	8	16
Tea	3	5	15

Room Rent perday Rs.	1000
Days accounted for	29 Days
Room rent amounts Rs.	29000
Service Bill amounts Rs.	39
Total Bill in Rs.	29039

Fig. 5.6 Pop-up window to prompt the user on error condition, with tips

AUDIT TRAIL CONTROL

Accounting Audit Trail

The accounting audit trail of the input subsystem should contain the following particulars:

- Identity of the person (organization) who was the source of data
- Identity of the person (organization) who entered the data into the system
- The time and date of the data entered

- The identifier of the physical device through which data is entered
- Account or record to be updated by the transaction
- Details of the transaction
- The number of the physical or logical batch to which the transaction belongs
- Similar events for validation of data-error correction, rejection, etc.
- Time of keying in a source document or an instruction at a terminal
- Number of read errors made by an optical scanning device
- Number of keying errors, identified during verification

By analyzing this data, error-prone or inefficient, input activities can be identified and remedial actions taken.

Existence Control

In case the master file is corrupted, the previous master file plus the input files can be used to rebuild the up-to-date master file. Accounting audit trail of the input subsystem is very important, as the same can be used to rebuild the input file. In case of input from a source document, it is essential to store the source document, for rebuilding the input, in case of a contingency.

PROCESSING CONTROLS

Processing controls provide reasonable assurance that data processing has been performed as intended, for the particular application and that all transactions have been processed as authorized, that no unauthorized transactions have been omitted, and also that no unauthorized transactions have been added. The following are some of the controls that can be used to review a computer application. Processing controls ensure the complete and accurate processing of authorized transactions.

Print Run to Run Totals

At each major stage during the processing of data in an application, it is necessary to track the data from one processing stage to the next and verify that the data was entered and processed, as it should have been. For example, a file of valid transactions, i.e. transactions that pass data validation and editing, can contain a control record showing the record count and control totals for the file. As the file is processed through a job (or job step) the computer can calculate a record counts and control totals for the transactions processed.

The computer calculated amounts are compared with the amounts in the control record. Agreements in the amounts, provide evidence that the processing was done accurately and completely. Disagreements indicate that a problem has occurred and needs to be investigated and rectified. Online or real-time systems, where transactions are not entered as a batch, can still utilize this technique, by establishing record counts and control totals over transactions entered during a specific time period, such as daily.

For applications where transactions are entered individually, as they occur, this concept is still of use. Files should contain information on the record count and control total, so that the computer can verify the completeness of processing as it progresses. Computer tape files would contain this information in a "trailer label" record that exists at the end of all data records on the tape. A disk file would contain this information in a control record. A program, creating the file, calculates and records the control information on the file. As a subsequent program processes the file, the computer calculates similar information and reconciles what it calculated with what was recorded on the file. Agreement in the amounts, indicates that all data was completely processed.

An example of the run-to-run total control implementation would be a cross-country race of ten miles, where there are five referees, each positioned at every two miles. One condition for the race is that people who are affected by a cold virus are not allowed to take part in the race. The referees are asked to put a tick mark against the name of the athletes as they cross the referees every two miles. An athlete is considered a winner only after the referees have given their statements. If an athlete has a tick mark in all the referees' statements, only then will he/she be declared a winner.

Here, the total number of competitors when the race starts is known and the number of people who complete the race is checked against the total number of competitors. The statements of the referees can be checked to find out if anyone is missing or at which stage an athlete retired from the race.

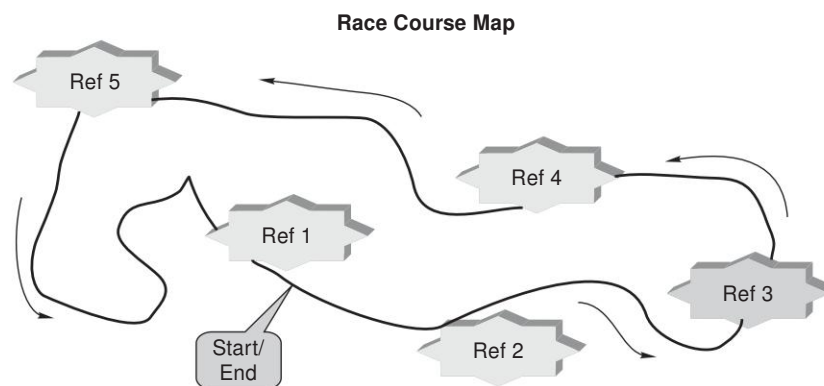


Fig. 5.7 Run-to-run total

A consolidated score sheet for the race would be like the table below. From the score sheet it is obvious that Jones, Jill and Steve have completed the race and the others have not. Moreover it can also be found in which stage they have quit the race. This run-to-run total control is used to track the data as it passes from one functional stage to another. We will be looking into this example as we move on to the other.

Table 5.1 Run-to-Run total

	Score sheet					Final result
	Referee 1	Referee 2	Referee 3	Referee 4	Referee 5	
Jones	✓	✓	✓	✓	✓	Complete
Jack	✓	✓	×	×	×	Incomplete
Jill	✓	✓	✓	✓	✓	Complete
White	✓	✓	×	×	×	Incomplete
Steve	✓	✓	✓	✓	✓	Complete
Walker	✓	✓	×	×	×	Incomplete
Snow	✓	✓	✓	✓	×	Incomplete

Lost and Rejected Entries

This control involves, matching transaction data with data in a master or suspense file. Unmatched items from both, the transaction data and master or suspense file are reported for investigation. For example, a payroll system may be designed so that each employee's time and attendance sheet can be matched with the employee's master pay record. Each time sheet, that does not match with a master pay record is reported, to determine whether or not it represents a valid employee and the master pay file also needs to be updated. Each master pay record that does not receive a match is reported, to determine whether a valid employee exists and a time sheet must be found or created so that the employee may receive his/ her pay on time. Also, master pay records with more than one time sheet are reported, which indicates that a duplicate time sheet exists for an employee.

Another example could be that before initiating a payment, a vendor's invoice could be matched with a file, containing records, detailing goods received. Invoices not matched could be reported to show that goods were not received and consequently, no invoices would be paid until a match was found.

Rejected transactions are controlled with an automated error suspense file. Using an automated error suspense file should control rejected transactions.

Transactions entered into this file should be annotated with:

- Codes indicating the type of data error
- Date and time, when the transaction was processed as well as the error identified, and
- The identity of the user who initiated the transaction

Record counts and control totals should be developed automatically, during the processing of erroneous transactions to the suspense file and should be used in reconciling the transactions that have been successfully processed. A control group should be responsible for controlling and monitoring the rejected transactions.

The suspense file should be purged of the related erroneous transaction as the correction is made. Record counts and control totals for the suspense file should be adjusted accordingly. The suspense file should be analyzed periodically to determine the extent and type of transaction errors being made and the age of uncorrected transactions. This analysis may indicate a need for a system change or some specific training, to reduce future data errors.

General controls should protect the suspense file from unauthorized access and modification, in order for the auditor to be able to rely on this control technique to reduce audit risk.

Let us go back to the example of the cross-country race. There are four participants who have quit the race at various stages. Referring to the table we find that Jack, White, Walker and Snow have quit the race. Now, it is important to know why these people have quit the race. If there is an athlete who has quit the race due to a cold virus which he had not revealed at the start of the race, then he will be held responsible, as the rule clearly states that he should not have taken part in the competition in the first place. In the same way, we can detect erroneous data in an application and then take necessary measures to avoid erroneous results. In this case, we could have a medical test, the day before the race. Let us say that some have quit due to the sweltering heat, then measures can be taken to hold the race at a time when the weather is pleasant and this will allow the athletes to perform better.

Mid-process Data Correction

Data processing controls are used to ensure the accuracy, completeness, and timeliness of data during either batch or real-time processing by the computer application. This control is used for reviewing application programs and related computer operations, to ensure that data is accurately processed through the application and that no data is added, lost, or altered during processing.

Checking the input data during processing and validation of data that is generated by the application system, are essential for assuring data integrity. Errors should be detected and corrected as soon as possible, in order to prevent the propagation of invalid data throughout the system and the potential contamination of the system data store. Care must also be taken to not allow the data to be modified when it is in the processing phase. Some instances where the data can be modified are during storage of application data, taking backup, etc.

Going back to the cross-country race, let us imagine that Snow has a twin brother Roger Thunder who is an average runner. Since they look identical, the brothers plan to let Roger complete the race after the third stage. It is possible that he may join the other runners at a sharp turn where there are no spectators. Roger will therefore, complete the race and the brothers will have a real good time enjoying the shared victory. Since such incidents should not take place, the organizers must ensure that the runners are monitored at every level and that the spectators are kept away from the runners, with a considerable distance between them. In the same way, data at different stages should be guarded to maintain the integrity of the data.

One way to maintain data integrity while processing would be, to minimize human intervention. Applications can take one-time inputs to automate the procedures that are to be repeated at regular intervals. For example, at the start of processing, a user or operator might have to use as an input, a parameter value to indicate whether a program is to undertake end-of-month or end-of-quarter procedures.

In some cases however, it might seem impossible to avoid some level of human intervention. In these situations, the program must provide clear instructions and clear feedback to the person who provides the input.

Before and After Image Processing

Computer data on a file, prior to and after a transaction is processed, can be recorded and reported. The 'before' and 'after' images make it possible to trace the impact that the transactions have on the computer record. In case of database management system (DBMS), logging before images of the database is a strategy, designed to facilitate rollback of the database. Each time a record is updated, its image before the update is logged. If a transaction fails before it commits all its changes to the database, it can be rolled back to the last commit point.

Cross Footing

In such kind of control, separate control totals can be developed for related fields and then cross footed at the end of a run. For example, in the case of a payroll application, the gross pay, deductions, and net pay can be cross footed and at the end of the run the application control should ensure that the net pay is gross pay minus the deductions.

Audit Trail Control for Processing Subsystem

The accounting audit trail should be designed so that the auditor will be able to trace and replicate the processing, performed on a data item that enters the processing subsystem. Following are some of the particulars that should form part of the accounting audit trail record of the processing subsystem.

- The process identifier, i.e. name and version number of the process
- Identity of the process that triggered the transaction and the condition that resulted in the transaction triggered
- The intermediate results and the value of any standing data item used
- The input and output data item values
- The date and time of the process
- Name of the user

Operation Audit Trail of the Processing Subsystem

Most of the resources utilized during processing are basically handled and managed at the operating system level. The event log, system log, and the security logs, store the information about these resources. Sometimes, the operating system allows the user/administrator to select the items, which are required to be the part of the audit trail record. In such cases, the user may be tempted to log too much data, but this may happen, only at the cost of processing. Some operating systems suspend user processes if the amount of data to be logged, exceeds the throughput capability of their logging facility.

Existence Control

Existence control in the processing subsystem can be achieved by many ways or a combination of different ways. One of the fundamental components of existence control is the replication of the components. For example, the dual

processor operating system is a kind of existence control. Another important logical existence control, which is built into many operating systems, is checkpoint/restart facility. In case of such control, if the program fails, for some reason, before it reaches normal termination, the processing will start from a mid-point, i.e. the point of failure, which is called the checkpoint. In such cases, the resources, used till the checkpoint of the processing, can be saved.

Output Control

Output of an application system can be in physical forms like printouts or in digital forms with different formats. From a management perspective, the output of any system is vital and the efficacy of the application system is judged or evaluated on the basis of the efficacy of the output. Since the output is the interface of the application with different entities, any flaws in the output will have a wide impact. Let us take the example of an internet banking system. In this case, if the user is able to obtain a report on the information related to the system or information about other users, then there is definitely a risk to the organization.

The basic task of the output control is to filter the output that users are permitted to see (inference control) and control the presentation of the output to the end users (presentation control).

Inference Control

Inference control precisely means that the users have access to the data items, but there are have restrictions on retrieving the inferences using such data. This is very important for a statistical database and it prevents four types of compromise that can occur to the information:

1. *Positive compromise*

In such a case, a user with some query or any user interface is able to know about a particular attribute of a person. For example, whether or not a person is married, etc.

2. *Negative compromise*

In this case, the user is able to know that a person does not have a particular attribute. For example, a person called "X" is not married, etc.

3. *Exact compromise*

The user determines the precise value of an attribute, possessed by a person i.e. how much loan "Mr X" has taken from the bank, etc.

4. *Approximate compromise*

The user determines approximately i.e. some range of the value of the attribute possessed by the person i.e. "the range of Mr X's salary."

Such compromises have an impact on the organization as whole, depending on the sensitivity of the information. The inference control can be broadly classified into (1) Restriction control and (2) Perturbation control.

Restriction Control

Such controls are implemented to introduce restrictions, so that the user cannot see the actual data, but can infer meaningful information from the aggregate data. Let us take the example of the following table:

Table 5.2 Restriction control

<i>Name</i>	<i>Sex</i>	<i>Position</i>	<i>Status</i>	<i>Salary</i>
Charles	M	Research Associate (RA)	Married (M)	10,000
Harry	M	Research Officer (RO)	Unmarried (U)	20,000
Lata	F	RA	U	15,000
John	M	RA	M	17,000
Raju	M	RO	M	18,000
Sandhya	F	Manager	U	21,000
Rashmi	F	Consultant	M	25,000
Yatin	M	Consultant	U	27,000

Let us assume that the query language that operates on this database, allows a full range of Boolean operators (AND, OR, NOT) and all sorts of statistical operations, viz. count, sum, average, etc.

Now suppose there is no inference control, how do we control the following illegal queries?

- How many unmarried female RAs are there in the organization?
- How many female consultants are in the organization?

Inference control is basically meant to limit the set of responses that will be provided to the users. This helps protect the confidentiality of data about persons in the database. In the above case, the inference controls could be of

any type like: 'do not respond to a query if less than K records satisfy the query, where $K = 2$ '. This means that if the number of rows returned in the query is less than two, i.e. one, then it should not be displayed. But such kind of a control can also be circumvented by a series of queries viz.

$K1$ = How many employees are RA or not RA? Answer = 8

$K2$ = How many employees are not female, unmarried and RA? Answer

Now from the two queries, you can infer that the number of employees who are RA, female and not married is one i.e. $K1 - K2$.

As you can see from the above, the rows returned in $K1$ and $K2$ are always more than one, so the constraints put above i.e. do not respond to a query if less than K ($K = 2$) records satisfy the query, will work.

Now, to apply further control, we can put in place, some more inference controls like, 'do not return a query if $K \leq n - k$, where K = number of rows returned and N = total number of rows in the array or in the table'.

There are ways to break this control, but the endeavor of the inference control is to ensure that users should not have easy access to restricted queries.

Perturbation Control

Perturbation control seeks to introduce some kind of noise into the statistics, calculated on the basis of records received from the database, so that it does not remain meaningful for unauthorized users. We can take the same example described earlier, but instead of putting a control like 'do not display the query if $K < 2$ ', we can display the record with some noise, so that the unauthorized user becomes confused and does not get the correct information and in the process, the confidentiality of the data is maintained.

Presentation Control

Presentation control is basically aimed at giving a reasonable assurance to the user that the data presented to the end-users are consistent and secure. This can be achieved with the help of the following controls:

- **Content Control:** Identifies the accuracy, age, relevance, filtering, and modification of the data presented. This can be achieved in different ways, by different control techniques. Currently, the role-based access control technique is used in the application logic to deliver the content to the user, depending on the role profile. In such a case, the content is filtered and customized as per the role of the user.

- **Medium Control:** Medium control is basically control over the medium through which the data is presented, i.e. paper, visual displays, voice, microform, etc. Sometimes important documents, viz. certificates, cheques/negotiable instruments, bonds, etc. are printed on preprinted stationery, as an output of the application program. In such cases, a detailed listing of generated forms should be compared with the physical forms received. All exceptions, rejections, and mutilations should be accounted for, properly.
- **Format Control:** There can be different formats of presentation. Like in the internet banking applications, the user is given the option to download the account statement in any format, viz. text, MS-Money, MS Excel, etc. In such cases, the risk is comparatively less, as this report is only accessible to the particular customer and any modification to this report will not be of much use to him/her. In the case of very sensitive reports, if the reports are allowed to be stored in any of the formats stated above, there is a chance that these can be modified offline and used for unethical/illegal purposes. Therefore, as far as possible, in the case of sensitive reports, these should not be allowed to be stored by the users in different formats. The print option should be made available, directly from the screen.

OTHER OUTPUT CONTROLS

- Output reports should be distributed according to authorized distribution parameters.
- Very sensitive reports should not be allowed to be printed in a remote network printer
- Reports that are distributed electronically should be accessible to users as per their role profiles
- Procedure for reporting and controlling errors, contained in the application program output, should be established. The error report should be timely and delivered to the originating department for review and error-correction
- The record retention should be as per the organization policy. Any governing, legal and regulatory guidelines should be included in the retention policy
- To provide assurance that sensitive reports are distributed properly, the recipient should sign a log as an evidence of the receipt of output
- While storing reports as a backup, it will be prudent to store the print file with the necessary digital signature. Storing the data, which

generates the reports, will not always work, as the application logic may change in the meantime.

Audit Trail Control for the Output Subsystem

Accounting Audit Trail

In case of accounting audit trail of the output subsystem, the chronology of events that occurs from the time the content of the output is determined to the time the users complete their disposal of output, is recorded in the audit trail record. The following important particulars should form part of the accounting audit trail:

- What output was presented to users?
- Who received the output?
- When was the output received?
- What action was subsequently taken with the output?

Operating Audit Trail

The following particulars should form part of the operating audit trail:

- The number of report pages printed or the volume of output requested by external users
- Printing time
- Display rates for the output, etc.

Such particulars can then be analyzed to determine whether or not an organization should continue to provide different types of output to users. This will also enable the organization to improve the timeliness of output production and optimize the amount of resources consumed in the generation of output.

Existence Control

The various controls that are required to ensure that the necessary output can be regenerated in case of any eventualities are as follows:

- Using large spool files, so they are overwritten less frequently
- Retaining the spool file for a longer period
- Checkpoint/restart facility for effecting partial recovery of the output
- Storing the data files and the related programs to generate the output at a latter date

OVERALL CONTROLS

- **Redundancy check:** In case of calculation routines, an additional calculation can be built-in with a different logic to compare the two
- **Stress limit:** Assumptions would be made, regarding the volume of transactions, number of concurrent users, number of files that can be opened simultaneously, etc. This control ensures that warnings are generated when these limits are reached
- **Backup and restore:** Backup and restore, at the application level should be thoroughly built into the application and only appropriate personnel should be allowed access to it

APPLICATION CONTROL AND COBIT

Application control in COBIT is described in the domain 'delivery and support,' under DS11, i.e. manage data. The high level control objective for this process is as below:

Control over the IT process of managing data that satisfies the business requirement to ensure that data remains complete, accurate and valid during its input, update and storage phases.

It is enabled by:

An effective combination of application and general controls over the IT operations.

And it takes into consideration:

- Form design
- Source document controls
- Input, processing, and output controls
- Media identification, movement, and library management
- Data backup and recovery
- Authentication and integrity of data
- Data ownership
- Data administration policies
- Data models and data representation standards
- Integration and consistency, across platforms
- Legal and regulatory requirements

AUDITING APPLICATION CONTROL

Review the Business Processes and Application System Documentation

- The first thing for an auditor to do, while conducting the application control review, is to understand the business process and related technology used to computerize this business process. This can be achieved by interviewing:
 - IT operations management
 - IT database administration management
 - IT applications development management
 - IT human resources/ training management
 - IT systems support management
 - Backup site security and administration management
 - Various user management for mission-critical applications

And by reviewing the following documents:

- Functional design specification
This document provides a detailed explanation of the application. An understanding of key control points should be noted during the review of the design specifications.
- User manual.
A review of the user manual gives an insight into how the system works. Often, control weaknesses can be identified from the review of this document.
- Technical reference documentation
This documentation helps in knowing the access rules and logic in the application.

Subsystem Factoring and Analyzing the Flow of Transaction Through the System

Once the auditor has a fair idea about the business process and the related technology, used to computerize that process, it is time to factor the system into subsystems. A subsystem is a component of a system that performs some basic functions needed by the overall system to enable it to attain its fundamental objectives. Subsystems are logical rather than physical components. The process of dividing a system into subsystems is called factoring.

Factoring is an iterative process that terminates when it is felt that the system has been broken down into parts, small enough to be easily understood and evaluated.

Let us take the example of a banking application, where there are various processes, viz. outward clearing, inward clearing, credit, cash payment, transfer payment, and backup, etc. Now, for factoring, we will either factor the application into modules or factor it further into submodules, i.e. modules within a module.

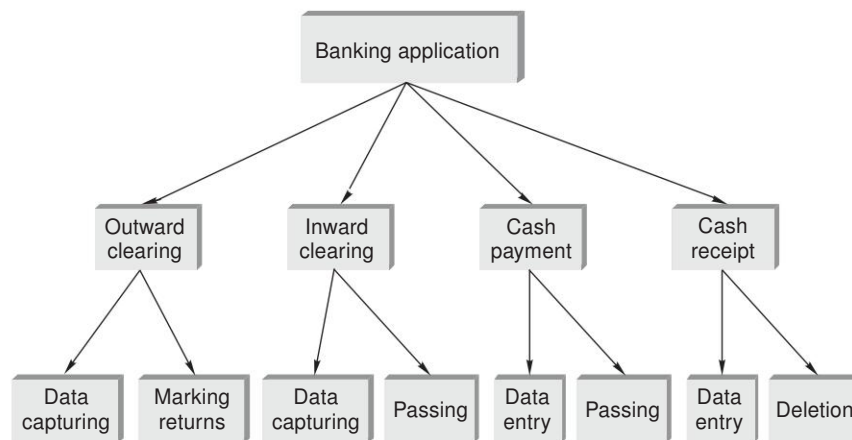


Fig. 5.8 Subsystem factoring

While factoring into subsystems, it should be ensured that each subsystem is internally cohesive and loosely coupled with other subsystems. All the activities performed by the subsystem should be directed towards accomplishing a single function. If this objective is achieved, then it will be easier for auditors to understand and evaluate the activities carried out by the subsystem. Normally, factoring is carried out by the auditors in a functional way, i.e. breaking the processes into activities and activities into tasks. This iteration goes on as long as the tasks remain discrete and cohesive, as well as loosely coupled with the main process. In some cases, factoring is done both, at the functional level and at the logical level. Logical level factoring is basically, breaking the application or processes into small logical units so as to reduce the dependencies among the small logical units and at the same time keep it cohesive and loosely coupled with the process/application.

Now, after factoring the system, the auditor should understand the functional controls, necessary for that particular factored subsystem and also try to match the implementation of these with functional controls in an IT environment. Although one-to-one matching is not required, as the business

processes would have been re-engineered before automation, yet it is important, from a control perspective to ensure that the basic and important controls are not bypassed, either during the business process re-engineering exercises or during automation. Auditors are supposed to comment on the adequacy and appropriateness of the control. Sometimes, auditors may also recommend a reduction of some redundant controls.

Let us look at one of the subsystems, i.e. the "inward clearing", break it into activities and find out the important controls required for such activities.

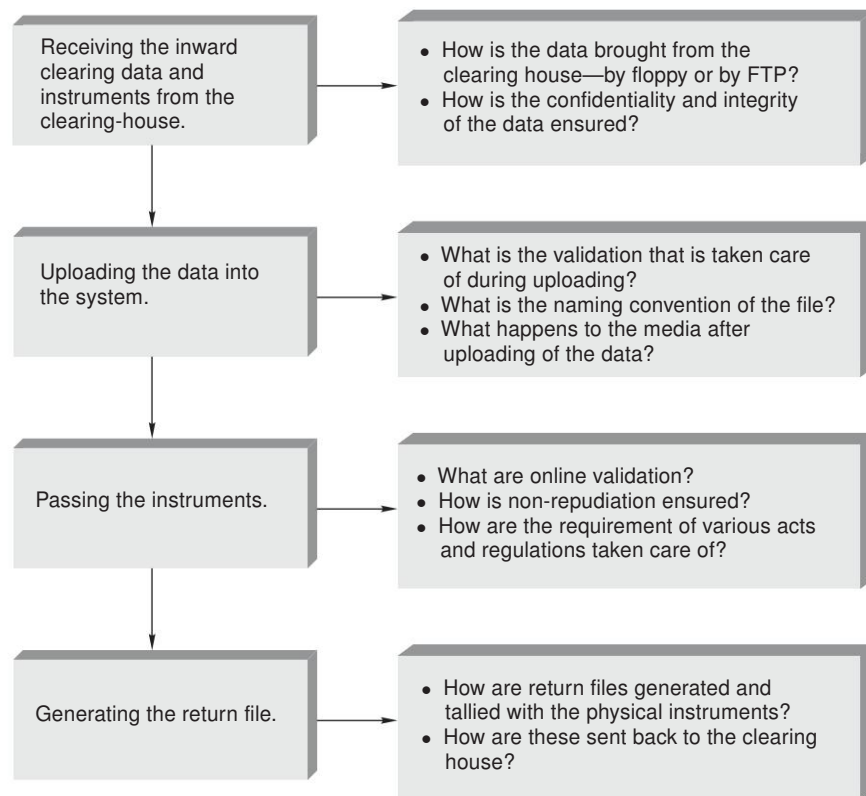


Fig. 5.9 Subsystem factorizing and recording functional controls

Inherent Risk Assessment

After identifying the control requirements for each process, the auditor needs to ascertain the inherent risk in that application, at that particular point of time. Such risk assessment can be based on many factors, which may include a combination of the following:

- Economic conditions
- Time elapsed since last review
- Changes in operation/environment
- Recent changes in key positions
- The age of the application
- Prior audit result
- Staff turnover
- Connectivity to outside world
- The quality of internal control

General Control Review

After taking a view on the inherent risk in the application, the auditor should review the general controls, related to the particular application and also other controls which indirectly affect the application. Some of the areas, which the auditor needs to look at, at this point of time, are:

- Physical security of servers and computers
- Uninterrupted power supply
- LAN cabling
- Fire protection measures
- The Annual maintenance contract for the application
- The organization and administration i.e. separation of duties, etc.

Some of the general controls can be reviewed by visiting the site and seeing their operation and some can be reviewed by observing the users performing the procedures. Activity reports should also be reviewed, to know about the overall health of the system and also to ensure that the activity is carried out only during authorized hours of operation.

Both, the inherent risk assessment and general control review of the application will give an indication to the auditor about the extent of substantive tests that are required to be done.

SUBSTANTIVE TESTS

Data Integrity Testing

Integrity testing is a set of substantive tests that examines the accuracy, completeness, consistency, and authorization of data, handled in the application system. This will indicate failures in input or processing controls.

Data integrity tests are of the following types.

Domain Integrity

Domain integrity testing, basically tests the field level input controls, in order to ensure that the data item has a legitimate value in the correct range or set. For example, the date field should not accept any illegal format, likewise the name field should not accept any numeric character. In such an exercise, the auditor needs to verify that the edit and validation routines are working satisfactorily.

Relational Integrity Levels

These tests are conducted at the data element and record-based levels. Relational integrity is enforced through the data validation routines, built into the application or by defining the input condition constraints and data characteristics, in the table definition, in the database stage itself. Sometimes the test can be a combination of both. For example, for ensuring that the Dearness Allowance (DA) is not be more than 20% of the basic pay for any employee, a few lines of codes can be written at the input level or constraints at the data definition stage can be specified, in case of an application using a backend Database Management System (DBMS).

Entity Integrity

Entity integrity ensures that no primary, key attribute of a relation is allowed to have null values. The primary key attribute must have a unique value. This can also be ensured at the code level or at the data definition level.

Referential Integrity

Referential integrity of the data can be ensured at the Database Management System (DBMS) level, if the application uses relational database at the backend. In the case of others, such kind of constraints can be achieved by writing a few lines of codes. In any case, whenever two or more relations are related through referential constraints (primary key and foreign key), it is necessary that references be kept consistent, in the event of insertion, deletion and updates to these relations.

Box 5.3**The ACID property in database Management System**

ACID stands for Atomicity, Consistency, Isolation and Durability. They are considered to be the key transaction processing features of a *Database Management System* (DBMS). Without them, the integrity of the database cannot be guaranteed.

In the context of databases, a single logical operation on the data is called a *transaction*. For example, a transfer of funds from one account to another is considered a transaction, even though it might consist of multiple tasks (debiting one account and crediting another). The ACID properties guarantee that such transactions are processed reliably.

- *Atomicity* refers to the ability of the DBMS to guarantee that either all of the tasks of a transaction are performed or none of them are. The transfer of funds can be completed or it can fail for a multitude of reasons, but atomicity guarantees that one account won't be debited if the other is not credited simultaneously.
- *Consistency* refers to the database being in a legal state, when the transaction begins and when it ends. This means that a transaction can't break the rules or *integrity constraints* of the database. If an integrity constraint states that all accounts must have a positive balance, then any transaction violating this rule will be aborted.
- *Isolation* refers to the ability of the application to make operations in a transaction appear isolated from all other operations. This means that no operation, outside the transaction can ever see the data in an intermediate state; a bank manager can see the transferred funds on one account or the other, but never on both—even if he ran his query, while the transfer was still being processed. More formally, isolation means the transaction history is serializable.
- *Durability* refers to the guarantee that once the user has been notified of success, the transaction will persist, and not be undone. This means, it will survive system failure, and that the database system has checked the integrity constraints and won't need to abort the transaction. Typically, all transactions are written into a log that can be played back to recreate the system to its state, right before the failure. A transaction can only be deemed committed after it is safely in the log.

TESTING THE APPLICATION SYSTEM

After the integrity testing of the data, the IS auditor should conduct application system testing, which *inter alia*, involves analyzing computer application

programs, testing computer application programs, etc. Methods and techniques, in vogue for such testing are as follows.

Snapshot

In case of a snapshot technique, the auditor will record the flow of designated transactions through logic paths within the program. For doing this, the auditor needs to have extensive knowledge of the IS environment. These kind of substantive tests are useful when the auditor feels that there are no strong internal controls in the organization.

Mapping

Identifies the specific program logic that has not been tested and analyzes the execution of the program, statement by statement. Such kind of an exercise is needed, to ensure the quality of the codes and find out the dead woods (unused codes), which can be removed to ensure greater efficiency. This exercise is also used to find out the potential exposures in the code.

Tracing and Tagging

The tagging and tracing approach, creates a "snapshot" of a pre-selected transaction (by the auditor), as it is processed through key points in the computer application. This allows the auditor to determine if the transaction has been recorded completely. An important advantage of this approach is that the audit work takes place concurrently, with the client's processing of regular transactions. The ability to randomly choose transactions, at any point, early in the processing cycle, provides evidence on the accuracy, completeness, and timeliness of processing in complex computer networks.

TESTING APPLICATION CONTROL

After testing the application system, the auditor should test the various controls in the application. The various techniques for testing the application controls are as follows.

Test Data

Test data involves developing and submitting fictitious transactions for processing, by an important computer application. Test data are developed to determine (1) whether or not control procedures that are built into the application are working effectively, (2) whether or not the computer is processing transactions correctly, and (3) whether or not all transactions and

master files are fully and correctly updated. The auditor only needs to test those controls that are important for evaluating a particular application. Since the auditor would not want to contaminate the client's data, a fictitious master file will be needed to run the "test" transactions. The *advantages* of test data techniques are as follows:

- The test data approach is useful for applications that process high volumes of transactions and in which computerized edit controls are considered important
- The test data techniques eliminate the need for source code review exercise
- This can be used as surprise basis
- The initial use can be limited to specific program functions thereby, minimizing scope and complexity

The *limitations* of the test data approach are as follows:

- Since the test data approach tests the computer program at a given point in time, any inferences about the correctness of processing, throughout the period, under audit, can be made only by ensuring that the application being used was the one that was in use throughout the period of the audit. Further, test data only tests the application program, not the clerical (data collection) aspect of the application.
- A common computer fraud is to add a code to a computer program, such that the additional code is executed only upon encountering specific criteria. Since test data, normally do not use live data, the specific criteria, necessary to trigger the fraud, may not be included in the test. Fortunately, process-tracing software is available which identifies program modules that were not executed by the test data. The auditor can then review these modules.
- The test data techniques do not test master files and master file records.

One of the variants of the test data techniques is the Base Case System Evaluation (BCSE). In this case, tests are conducted with a set of test transactions, containing all possible transaction types. These are processed through repeated iterations during system development testing, until consistent and valid results are obtained. These results are called the base case. When subsequent changes to the application occur during maintenance, their effects are evaluated by comparing current results with base case results.

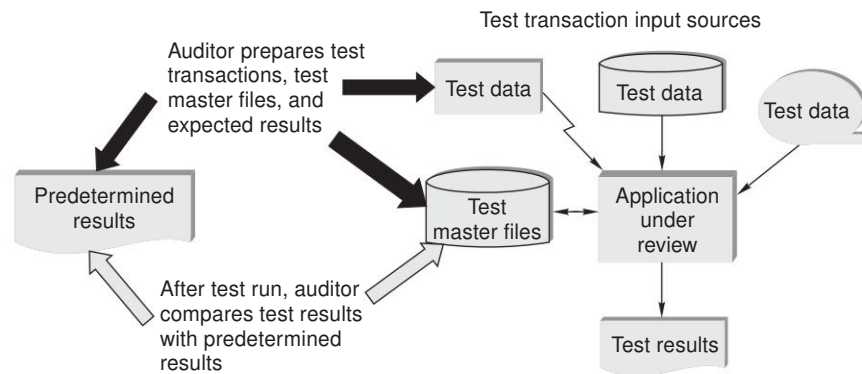


Fig. 5.10 The test data technique

Integrated Test Facility (ITF)

The integrated test facility is designed to overcome a major limitation of test data which confines the test results to a particular point in time. In utilizing an ITF approach, the auditor develops a "dummy company" against which transactions are submitted by the application. The salient features of ITF method are as follows:

- Data processing does not know when the computer application is being tested. Audit objectives are similar to the test data

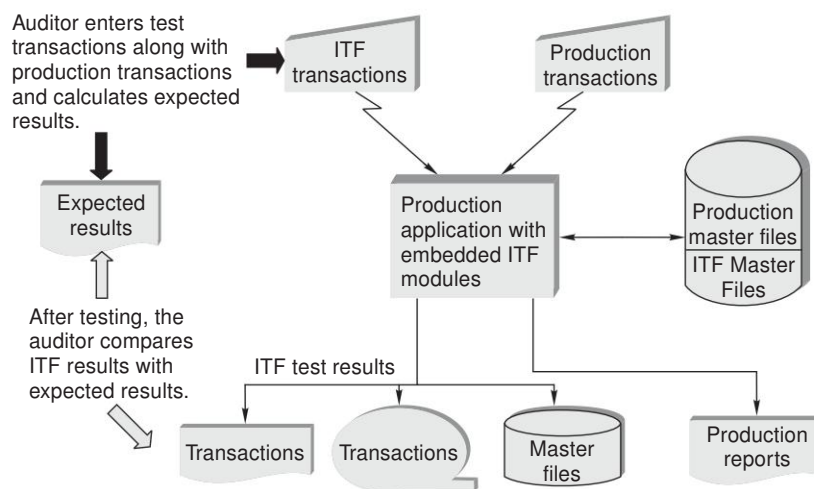


Fig. 5.11 The ITF technique

- An ITF also has the ability to detect errors that might have been caused by changes, made to the program during the year, since the computer-generated output will differ from the auditor's expectations
- Since test transactions are run against the "live" program, there is a potential problem that the fictitious data could update the general ledger accounts. One solution to this problem is to submit reversing journal entries to reverse the fictitious transactions. Another is to design the ITF such that, the transactions of the "dummy entity" are "peeled off" and are not used to update the accounting record

CONCURRENT PROCESSING METHODOLOGIES

These consist of audit modules or other programming, built by the auditor, directly into important computer applications to select and monitor the processing of data. As such, these techniques are likely to receive increased use in complex and interconnected computer applications. Apart from the 'tagging and tracing' approach, which has been discussed earlier, the other concurrent processing methodologies are as follows.

The Systems Control Audit Review File Approach (SCARF)

This approach differs from tagging, and tracing, in that, it requires the auditor to install codes into the computer application to select transactions which meet specified criteria, such that all selected transactions are written out to a file for subsequent audit review. Another use of this approach is to select for review, all transactions that are entered by overriding edit controls.

Embedded Audit Modules (EAM)

These consist of codes, added to client programs by the auditor. They are useful whenever the auditor wants to gather information for further testing. Their primary purpose is to assist in either:

- Performing tests of account balances or
- Gathering evidence on the integrity of processing and related control

Disadvantages of Embedded Audit Module (EAM)

The EAM approach has two significant disadvantages, viz. operation efficiency and the integrity of EAM itself.

Operational Efficiency

The presence of an audit module, within the host application, is itself an overhead and will consume some computing resources. One way to relieve the system of this burden is to design modules that may be turned on and off by the auditor. Again, doing so will reduce the effectiveness of the EAM as an ongoing audit tool.

Verifying the EAM Integrity

This approach is not a viable audit technique in environments with a high level of program maintenance. When host applications undergo frequent changes, the EAMs, embedded within the host will also require frequent modification. So the integrity of the EAM may be affected, which will directly affect the quality of the audit process.

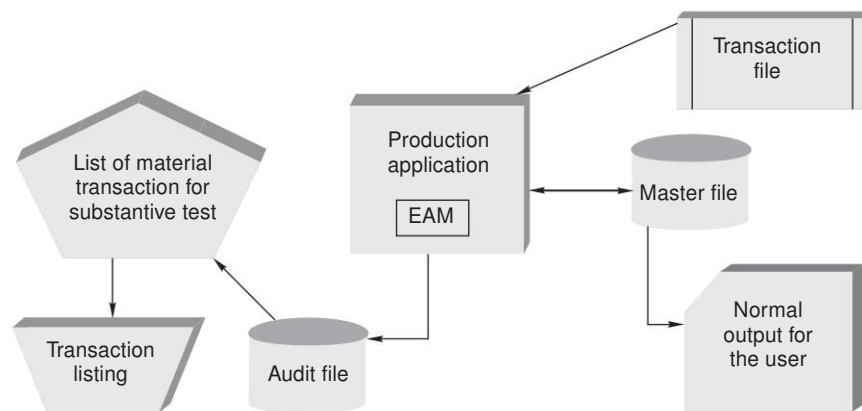


Fig. 5.12 Embedded Audit Module (EAM) Techniques

Box 5.4

Storing reports for backup

An organization decides to discontinue the generation/printing of various reports, as the work flow system, allows the screen viewing of the report by various functionaries, as per their role profiles. The data of the application program, which is used for generation of the program is stored with due care and the retention of the data is done as per the retention policy of the organization. Things were going smoothly for some years and the organization was on the way to transform itself into a paperless

(Contd)

set-up. Suddenly, there arose an urgent requirement for some old reports for certain legal purposes. The data for that period was retrieved and the current application was used to generate the report, but—the application logic had changed in the meantime and the new application did not recognize the old data, any more. The data is garbage for this particular application. What should be done? How should the report be generated? Should a program be written to generate the report? Will this be acceptable, legally? Should we have stored the application along with data as a backup? Our application is very thick and changes very frequently. So how do we manage to store the data with the application every time? Or else will it be better to store the print file of the report with digital signature as a backup instead of the data alone?

CONVERSION AUDIT

We all know that the Information Technology environment is very dynamic and the technology, which is current today, can become obsolete in no time. Keeping pace with the latest technological developments is very difficult for an organization. But there are very few alternatives to that. When the technology becomes obsolete, the organization can least afford to keep its legacy application, as it is, because of many reasons, viz. heavy maintenance cost, lack of technical resources, no more hardware support from vendors, problem in integrating new utilities, which are developed in new technologies and greater flexibility, provided by the current technology. So, there is a definite need for acquiring new technology. But what would happen to the data, which the organization has been storing for years? They can least afford to throw it away or ignore it. This data needs to be integrated with the new technology and hence, arises the primary need for data conversion from the old system to the new one. Let us take the example of a legacy application in a bank, developed in MS COBOL with Btrieve files at the backend and that has been running for the last ten years in many branches, as a Total Branch Automation package (TBA). Now, the bank takes a decision to opt for a core (centralized) banking solution which uses Oracle Database Management System at the backend. In this case, it is vital for the bank to convert the old data in Btrieve format to the relevant tables, in Oracle. Although most of the data conversion requirement is because of this, there are also other reasons for data conversion, viz.:

- Initial computerization of the organization from manual operations. In this case, there is a requirement for conversion of manual data to computerized data

- Rolling out of branches to a computerized application. Manual data need to be captured in the new computerized application
- Sometimes, change in the hardware, necessitates change in the operating system, Database Management System (DBMS) and application system. Consequently, there is a requirement for data conversion from the old system to the new one
- When the organization goes for an Enterprise Resources Planning (ERP) solution, there is a need to convert the old data to the new ERP system
- Sometimes, for integration of any new utility or module with the old application, there is a need for integration of data

Control Requirement of Conversion

Sometimes in the rush to computerize or switch over to a new application, the conversion process is ignored. As a result, the organization starts with a lot of overheads in the new application and there is also the possibility of occurrence of frauds, using this route. Therefore, the control requirements for conversion are very important, which organizations can least afford to ignore. Some of the requirements are listed below.

Data Integrity

Data integrity is the first and foremost requirement for any organization. It is not only required by the decision makers of the organization, but also by the stakeholders of the organization. Since in the conversion phase, the data will be handled at various stages, by various entities and processes, the entire process of data conversion should therefore, be properly planned and well-documented.

Data Validation

Data validation i.e. the basic boundary control and the input control of the application will be bypassed during the conversion, as special routines or special programs will be prepared for populating the basic data. It should therefore, be ensured that the required validation, as per the business logic, is never overlooked.

Calculated Fields

Calculated fields are very important from a conversion point of view. These fields are basically data items, which are calculated from other fields. For

example, the net salary is a calculated field, which is calculated from 'basic from net earnings minus the net deductions.' In case of conversion, since the calculated fields are directly taken into the new application, it is very important to keep the integrity of these, intact. Therefore, it is advisable to run a separate routine after the conversion, to ensure that the integrity of the calculated field is maintained. This routine should essentially have the same logic as the old application, for generation of the calculated field. The auditor, of course, should conduct further substantive tests, using various tools to verify the correctness of the calculated field.

Audit Trail

Audit Trail is the primary source for building the profile of the past behavior of the user. Now, when the past data is transferred from the old system to the new system, the past behavior should also be transferred. Care must be taken to ensure that the linkage between the past data and the past behavior remains intact and that there is continuity in the past behavior, in the new application.

Balances in the Transit/Parking Accounts

Balances in the transit/parking accounts are very important as they can be used as a means for perpetrating financial fraud. Therefore, the balances and more so, the unreconciled balances in these accounts, should be carefully transferred from the old to the new applications. It is advisable to get appropriate management approval before freezing the balance and transferring it to the new account. All these documents should be kept as permanent records for evidence purposes.

Master Data

Master data preparation is one of the fundamental requirements in the entire conversion process. This is because of the dependency of these data on the rest of the data. Any inconsistencies in these data will therefore, affect the entire database. The usual practice in the industry is to take the manual print out of the master files from both, the old and new applications and compare these manually, before starting the live run of the new application.

Conversion Audit Process

The basic objective of the conversion audit is to ensure that the data integrity is not lost or diluted while converting from one application to another. The auditor's role is to collect and evaluate necessary evidence to assure the

management about the correctness and purity of data in the new application. In fact, as per the normal industry practices, the live run of the new application is only commenced after the conversion audit has been completed or is done on a priority basis, as soon as the live run is commenced. The various steps involved in the conversion audit process are as follows.

Compliance Testing

Comparing the Master Listing Data Sheets

The first and foremost requirement for the auditor is to generate the listing of master files from the old and the new applications and compare them. The old application could either be computerized or a manual application. In both the cases, the same procedures for comparing the master files should be carried out. In fact, the auditor will evaluate the comparison, which was supposed to have been done by the organization. In such cases, the auditor should ensure that the data comparison sheets are authenticated by an authorized official and kept in safe custody.

Outstanding in the Parking Accounts

Outstanding in the parking accounts in case of a banking organization, it should be ensured that all the outstanding entries in the parking accounts and all other important accounts are entered in the new system. Some of the important accounts which the auditors should check for this purpose are:

- Bankers' cheque
- Sundry creditors
- Suspense
- Overdue term deposit
- Bills, cheque discounted, partywise
- Gift cheque
- Bills payable A/c. – draft
- Draft ex-advice A/c.
- Clearing A/c.

The auditor should again compare the balances of these accounts in the old and new systems.

Transaction Data Transfer

There are usually two ways of transferring transaction data to the new system. Either, only closing balances are transferred or the entire data from the old system is transferred to the new system. In the case of transfer from pure

manual operation to computerized operation, usually the closing balances of all the accounts are transferred, while in the case of transfer from one computerized to another computerized application; the entire history data is transferred to the new system. In the latter case, the auditor has to conduct substantive tests, for arriving at various control totals and matching these with those of the old system. However, in the case of the former, the authenticated closing balances of the old system, as on a cut-off date, should be matched with the opening balances of the new system.

Generation of Balance Sheet

The auditor should ensure that an account balance sheet of the organization (branch) is taken, as on the cut-off date of conversion, from the manual/ automated system to the new system. This balance sheet should use the data from the old application. At the end of conversion, before entering any transaction data, another balance sheet should be generated by the new system and compared with that of the old system.

Substantive Testing

The amount of substantive testing, the auditor should conduct is again, dependant on the resultant comfort of the compliance testing. If the result of compliance test is not very satisfying, then the auditor may choose to conduct various substantive tests. The purpose of this kind of a test is to assure the management about the data integrity during the conversion process. The various substantive testing procedures that are used by the auditor are as follows:

Control Total

Generation of control totals is basically a detective control, where the auditor, either write routines or use certain tools to calculate various control totals from both the applications (convertee and converted) and compare the results.

Check Sum

Under this method, check sum is generated for various numeric fields of both, the old and new systems and then compared.

Calculated Field

As has been discussed earlier, such totals are calculated from other fields. In case of data conversion, since such fields are directly populated to the new application, no field level or record level validation may have been taken into consideration. Therefore, the auditor may write routines to recalculate the value of the calculated fields and compare these for ascertaining their correctness.

Box 5.5**Audit tips for a bank auditor on conversion audit**

- Check whether the following activities have been completed:
 - Creation of days
 - Calendar updating
 - Declaration of holidays
- Whether or not stopped cheque details have been loaded?
- Whether or not monthly products up to the previous month have been loaded.
- Whether actual limit and interest rate for overdraft/term loan/cash credit accounts have been entered?
- In case of overdraft/cash credit account, whether accrued interest till the cut-off date has been entered?
- Whether interest paid date and amount captured for term deposits?
- For *term loan*, whether limits and classification of accounts has been entered properly?
- Whether *charges* account is posted as per classification accounts heads and subheads as per charges a/c format?
- For interest/exchange/commission/discount, whether accounts are posted subheadwise?
- In case of interest account, whether posted as per income or expenditure?
- In R/D accounts:
 - Whether date of instalment paid, in respect of all accounts has been entered
 - Whether interest provision has been done up to the last quarter.

Checklist for auditing the application control**A. Boundary Control**

1 = Not satisfied, 2 = Unsustainable,

3 = Needs improvement, 4 = Satisfied

1. Does the application come up directly by booting the computer or by going to the operating system (CLI) and invoking some command or clicking some icon? If answer is direct booting, answer question 2 or question number 4.
(Browser-based applications are not covered)

(Contd)

230 Information System Audit and Assurance

2. Is there any control for not breaking the login script/ batch file which takes the user directly to the application (auditor should try to break it by pressing Control + C or Control + Break) (1 = No control; 4 = sufficient control)	1	4			
3. Are the login names, used in the operating system to login, the same for all the users or are these different for different levels of users?	1	2	3	4	
- If the names used are the same, then check the business requirements for such an arrangement and also the user rights of the operating system level user. If the user has no supervisory right, then put the score as 2 and if he/she has supervisory rights, put the score as 1. - If the names used are not same, or there are many users at the operating system level, then get a user list and check their access privileges, compare that with the business requirement, as approved by the user management and also map the operating system ID with the application ID to check for inconsistencies. It may happen that a normal or low-level user in the application system has a supervisory access to the operating system. Such things are not desirable from the security and control perspective. Depending on the state of the affairs, give a rating in the range of 1 to 4.	1	2	3	4	
4. If the computer boots locally and then goes to the operating system interface then, answer the questions from 5 to 7.	1	2	3	4	
5. Evaluate the access control in the local machine. The access to the local machine should be secure and in accordance with the security policy and procedures of the organization/bank. Depending on the label of security, give a rating from 1 to 4.	1	2	3	4	
6. Evaluate the anti-virus measures taken by the organization to ensure that the network doesn't get infected, because of any of the poor practices at the client level. Depending on the evaluation, give a rating from 1 to 4.	1	2	3	4	

(Contd)

7. Evaluate the access rights of the user and ensure that it is as per the organization's IT security policy and procedures. Depending on the evaluation, give a rating from 1 to 4.	1	2	3	4		
8. Evaluate the creation and maintenance of user ID and password in the application system.	1	2	3	4		
(a) Does the application system have a separate user ID creation module or does it take the operating system user ID and allocate the necessary resources?						
(b) Does the software allow creation of duplicate user IDs and Passwords?						
(c) Does the application encrypt the passwords and store them in an encrypted form?						
(d) Are the passwords displayed as and when keyed in?						
(e) Does the application give prompt about an invalid user ID, after entering the user ID or after entering the pair (user ID + password)?						
(f) Are there any locking facilities for locking the password after three successful login attempts?						
(g) Is there any restriction on the minimum length and combination of character in the password?						
(h) Are the passwords stored in a backend database without encryption?						
(i) Does the application remember the history of the password?						
(j) Does the application force the user to change the password at the periodical intervals?						
(k) Does the software map the user ID to the functional designation and position? (Depending on your evaluation, give a rating from 1 to 4.)						
9. Evaluate the backend maintenance of the user ID and password file.	1	2	3	4		
(a) Does the user have the right to change the password file at the backend?						
(b) Does the DBA have the power to change the password file from the backend without going to the menu (not desirable)?						

(Contd)

232 Information System Audit and Assurance

(c) When the user ID and password are deleted, are they deleted physically or logically?				
(d) Can a user ID be created without a password?				
(e) Does the software allow logical division of inactive users after a certain period of time?				
(f) Is there any manual authorization process for creation or division of user ID?				
(g) Are there any dummy user accounts (maintained by professional vendors, maintenance professional, etc.)? (Depending on the evaluation, give a rating from 1 to 4.)				
10. Is there any menu management in the software? If yes,	1	2	3	4
(a) Who manages the menu (menu should not be managed by a normal user)?				
(b) Menu is best on role or individual? (Depending on the evaluation, give a rating from 1 to 4.)				
11. Verify the audit trail of boundary subsystem. The audit trail should contain the following particulars:	1	2	3	4
• Identity of the user-to-be of the system				
• Authentication of the information supplied				
• Resource requested				
• Action privileges requested				
• Terminal identifier				
• Start and finish time				
• Number of login attempts				
• Resource provided/ denied				
• Action privileges allowed/ denied (Depending on the evaluation, give a rating from 1 to 4.)				
12. Verify the existence control in the boundary subsystem and give a rating from 1 to 4.	1	2	3	4
B. Input Control				
13. Field label input control	1	2	3	4
Take some data entry forms and check the following:				

(Contd)

(a) Has any sequence check been implemented, as required?				
(b) Has any limit check been implemented, as required?				
(c) Has any range check been implemented, as required?				
(d) Has the input data been validated against a predefined set of values?				
(e) Has the master reference been implemented properly?				
(f) Has any size check been implemented? (Depending on the evaluation, give a rating from 1 to 4.)				
14. Record level input control	1	2	3	4
(a) Has any reasonableness check been implemented as per requirement?				
(b) Have the numeric fields been validated against correct signs? Has the valid sign numeric control been implemented at the record level?				
(c) Is there any control at the record level, to control the size of the record?				
(d) If logical records are spanning more than one physical record then are the sequence numbers correctly stored? (Depending on the evaluation, give a rating from 1 to 4.)				
15. Batch level input control	1	2	3	4
(a) If the input of data is through batch upload, does the software have controls to ensure that all the entries in the batch have been uploaded without any omission/ commission i.e. control totals have been reconciled?				
(b) Have transaction type controls in the batch process been implemented?				
(c) Check whether each input record in the batch is given the unique serial number that has been assigned to the batch. (Depending on the evaluation, give a rating from 1 to 4.)				

(Contd)

234 Information System Audit and Assurance

16. File level input control	1	2	3	4			
If input is taken from a different file please check the following:							
(a) Is there any input validation, to check the correct name of the file?							
(b) Is there any control to check the correct version and generation number of the file?							
(c) Has the authenticity of the file been verified at the input stage by taking some control total? (Depending on the evaluation, give a rating from 1 to 4.)							
17. Other input level controls	1	2	3	4			
(a) Verify the consistency of the user inputs. Are two users assessing the same record at the same time?							
(b) Verify if the inputs can be captured for various conditions.							
(c) Verify the maker-checker concept of the input. (Depending on the evaluation, give a rating from 1 to 4.)							
18. Data entry screen design	1	2	3	4			
(a) Check whether the screens are unclotted and symmetrically balanced?							
(b) Whether there are logical breaks between screens, in case where there is a requirement of multiple screens?							
(c) Is there any space in the screen for displaying messages like 'help', 'error', etc.?							
(d) Is the screen organization, consistent across the entire application?							
(e) Is the caption of the screen, context-specific?							
(f) Is the caption blinking? (not recommended)							
(g) Is the caption in a font bigger than other items in the data entry screens?							
(h) Is there any caption to vary specific field?							
(i) Is the confirm option set to 'yes' (recommended option is 'no')?							
(j) Is there any atomic skipping new field? (not recommended)							

(Contd)

(k) Are the colors used in the screen RYGB (Red, Yellow, Green, and Blue (recommended))? (l) Are the colors distinct and consistent across the activities? (m) Are there any options for color blind users (using uppercase and lowercase text to differentiate capitals from the data entry items)? (n) Is the help section context-specific and granular? (Depending on the evaluation, give a rating from 1 to 4.)				
19. Audit trail for input	1	2	3	4
Check the audit trail file and evaluate the following:				
(a) The accounting audit should contain the following particulars: • Identity of the person (organization), who was the source of the data. • Identity of the person (organization) who entered the data into the system. • The time and date of data entered. • The identifier of the physical device through which data is entered. • Account or record to be updated by the transaction. • Details of the transaction. • The number of the physical or logical batch to which the transaction belongs. • Similar events for validation of data-error correction, rejection, etc. • Time of keying in a source document or an instruction at a terminal. • Number of read errors made by an optical scanning device. • Number of keying errors identified during verification.				
(b) Whether the audit file can be accessed by usual users?				
(c) Whether change in the audit file is locked? (Depending on the evaluation, give a rating from 1 to 4)				

(Contd)

C. Processing Control

20. Does the software have adequate controls to ensure that all transaction inputs have the updated relevant files?	1	2	3	4
21. Are there adequate procedures for investigation and correction of differences, identified by the controls, over update of completeness and accuracy?	1	2	3	4
22. Are such corrections approved?	1			4
23. Is there any restart facility for batch jobs if they terminate abruptly? Are there controls to ensure that no errors are introduced during restart?	1	2	3	4
24. Is the user ID of the person who executes the batch jobs, embedded in the transaction?	1	2	3	4
25. Is the application a day-end and day-begin operation? If yes, can the day-begin operation start without the day-end operation?	1			4
26. Does the application allow direct debit to journal ledger head. If yes, whether this is controlled through proper user parameter values and exception reports generated?	1	2	3	4
27. Can the transactions of the previous day be booked after the day-end operation?	1			4
28. Can the system allow concurrent transactions for two different dates?	1			4
29. If an update occurs in more than one file or table and the process is interrupted, is there a proper roll back?	1	2	3	4
30. Does the software permit transaction on a holiday?	1			4
31. Can the reopening of the close-day be done by a normal user?	1	2	3	4
32. Does the audit trail for the processing control has the following items?	1	2	3	4
• The process identifier i.e. name and version number of the process				
• Identity of the process that triggered the transaction and the condition that resulted in the triggered transaction				
• The intermediate results and the value of any standing data items used				

(Contd)

• The input and output data item values • The date and time of the process				
33. Is the existence control like a dual possessor in the server? Are check-point, restart facilities in the OS and application present and functioning properly?	1	2	3	4
D. Output Control				
34. Verify that the application maintains adequate control over security items such as DDs/ pay orders/ branch advises, etc. Are they reconciled and are exceptions identified and reported?	1	2	3	4
35. Is the generation of exception reports mandatory (i.e. link to the day end process (recommended))?	1	2	3	4
36. If the output has more number of pages and if printing is interrupted, is there any provision to restart the printing from that page?	1	2	3	4
37. Verify whether generation of output is on a need-to-know basis.	1	2	3	4
38. Check the adequacy of control over print queue/ spool.	1	2	3	4
39. Is the network printer which generates important output kept in a secure place?	1	2	3	4
40. Has the restriction control been properly implemented?	1	2	3	4
41. Evaluate the adequacy of the control for the pre-printed stationeries.	1	2	3	4
42. Check whether sensitive reports are allowed to be stored by the user in different formats (not recommended).	1	2	3	4
43. Check whether sensitive reports are allowed to be printed in the remote network printer.	1	2	3	4
44. Check if the reports which are distributed electronically are accessible to the users as per their role profiles?	1	2	3	4
45. Check if the error reports are delivered to the originator department promptly, for review and corrections?	1	2	3	4

(Contd)

238 Information System Audit and Assurance

46. Check if the record retention policy is in accordance with the legal and regulatory guidelines?	1	2	3	4			
47. Is there any procedure for taking a receipt for distributing sensitive reports as evidence of receipt of the output?	1	2	3	4			
48. Check audit trail of the output systems and see whether it contains the following parameters:	1	2	3	4			
• What output was presented to users?							
• Who received the output?							
• When was the output received?							
• What action was subsequently taken with the output?							
• The number of report pages printed or the volume of output requested by external users							
• Printing time							
Display rates for the output, etc.							
49. Check whether the following existence controls have been properly implemented:	1	2	3	4			
• Using large spool files so they are overwritten less frequently							
• Retaining the spool file for a longer period							
• Checkpoint/restart facility for effecting partial recovery of the output							
• Storing the data files and the related programs to generate the output at a later date							
E. Authorization Control							
50. Does the software prevent the same user from performing both the functions of entering the transaction and verifying it?	1			4			
51. If manually approved transactions are authenticated by the input of the password are passwords adequately controlled?	1	2	3	4			
52. If the transaction is authorized by the software itself, is the application logic sound enough to ensure that such authorizations take place as expected?	1	2	3	4			
F. Other Application Controls							
53. Are the application parameters changed with proper authentication and dual control?	1			4			

(Contd)

54. Is there any provision for marking lost/stolen draft in the system, for both, single and bunch leaves and without amount?	1	4		
55. Is there any access to signature database outside the application software? (that is, adding signature from external file should be avoided).	1	4		

The checklist given above is not very comprehensive and does not contain perimeter controls, general controls, database controls and the controls, related to the operating systems. This checklist can be customized for specific needs of the organization, by adding inputs on specific functional requirements. The authors are of the opinion that the auditors should lay stress on the "with computer" or "through the computer" approach of audit, using different Computer Assisted Audit Tool and Techniques to give opinion about the functioning of an application system. A checklist can be an aid, but not a solution.

SUMMARY

Application control is a very vast area. Although the entire gamut of application control could not be covered in this chapter, we have tried to cover most of it. The rest i.e. the controls over web-based applications, has been covered under the chapter "Internet banking risks and control". In this chapter, we discussed the definition of application system from a control perspective and went ahead to describe various types of applications, depending on both, function and usage. We factored the application system into various subsystems viz. boundary, input, processing, operating system, DBMS and output and discussed the risks and controls of each subsystem. While the risks and controls of an operating system has been covered in a separate chapter, the basic of DBMS control was covered in this chapter. After covering the controls in all the subsystems, we discussed the application control as per COBIT. The auditing of the application system was covered in detail with the steps, required to conduct the audit and various methods, used for testing application systems and application controls. We also discussed the risks and controls of the conversion process i.e. conversion from one application to another. At the end, we have given a generic checklist for auditing application control, which can be used by the auditor as a reference.

REVIEW QUESTIONS

1. What are application systems? Discuss the various types of application systems, depending on usage and architecture?
2. What are web-based applications? Why are these called thin client solutions? What are the advantages and disadvantage of these solutions?
3. Describe the lifecycle of an application system.
4. What are the objectives of a boundary subsystem? Describe the audit trail and inference control for the subsystem.
5. Describe the field level input control in an application system, with an appropriate example.
6. Describe the record level input control for an application system with an example
7. Describe run-to-run total and mid-process data correction with suitable examples.
8. Describe the restriction control in an application system with examples.
9. Describe various risks involved in the output subsystem of an application system and describe the required controls.
10. Describe the application conversion process and the various concomitant risks and necessary controls.

MULTIPLE CHOICE QUESTIONS

1. Control, designed to validate a transaction at the point of data entry is called:
 - (a) Re-calculation of batch total
 - (b) A record count
 - (c) A check digit
 - (d) Re-calculation of hash total
2. Which of the following is not a file label input control?
 - (a) Header label
 - (b) Expiry date check
 - (c) Sequence check
 - (d) Version check
3. Which of the following statements is not correct?
 - (a) Only successful transactions are recorded on transaction log.
 - (b) Unsuccessful transactions are recorded in an error file.

- (c) Transaction log is a temporary file.
- (d) A hard copy transaction listing is provided to the user.
- 4. Which of the following is the most appropriate for an application system?
 - (a) A group of computer systems.
 - (b) A group of computer system and related manual system.
 - (c) A computer system, written in high level language.
 - (d) A set of interrelated components, designed for performing a particular business process.
- 5. Which of the following is true about an audit trail?
 - (a) Audit trail contains the transaction details.
 - (b) Primary source for building the profile of past behavior.
 - (c) Required by auditors for conducting audit.
 - (d) It maintains only the record of each event within the system/subsystem.
- 6. The product code will raise from 200–500. Any code outside this range will be rejected by the system. Such kind of an input control is:
 - (a) Sequence check
 - (b) Limit check
 - (c) Parity check
 - (d) Range check
- 7. Which of the following is an example of a record label input control?
 - (a) Sequence check
 - (b) Limit check
 - (c) Range check
 - (d) Reasonableness check
- 8. Which input validation check would detect a payment made to a non-existent vendor?
 - (a) Missing data check
 - (b) Range check
 - (c) Validity check
 - (d) Numeric/alphabetic check
- 9. Which of the following would best ensure the proper updating of critical fields in the master record?
 - (a) Field check
 - (b) Control totals
 - (c) Reasonableness check

242 *Information System Audit and Assurance*

- (d) Before and after maintenance report
- 10. The primary reason for enabling software audit trails is to:
 - (a) Improve response time for users.
 - (b) Establish accountability and responsibility of processed transactions.
 - (c) Improve system efficiency.
 - (d) Provide useful information to auditors for tracking transactions.
- 11. Which of the following, best describes an Integrated Test Facility (ITF)?
 - (a) The utilization of hardware and/or software to review and test the functioning of a computer system.
 - (b) A method of using special programming options to permit printout of the path to a computer program, taken to process a specific transaction.
 - (c) A technique that enables the IS auditor to enter test data into live computer, run for the purpose of verifying correct processing.
 - (d) A procedure for tagging and tracing transactions and master records that are used by an IS auditor for tests.
- 12. The goal of batch control is to ensure that during processing:
 - (a) Transactions are not omitted.
 - (b) Transactions are not added.
 - (c) Transactions are processed more than once.
 - (d) An audit trail is created.

DISCUSSIONS AND RESEARCH QUESTIONS

1. Define data integrity testing and describe the types of data integrity tests.
2. What kind of a control is the Embedded Audit Module (EAM)? Describe the various variants of EAM.
3. What is the difference between a testing application program and testing application control. Name the different types of techniques used in both.
4. Output controls ensure that output is not lost, misdirected or corrupted and that privacy is not violated. What are some of the output exposures, or situations where output may be at risk?
5. What are the primary objectives of batch control?
6. Classify each of the following as either a field, record or file level control:
 - (a) Limit check

- (b) Version check
- (c) Validity check
- (d) Sign check
- (e) Sequence check
- (f) Size check
- (g) Reasonableness check

EXERCISES

1. Identify the type of input validation techniques for the following inputs to the payroll system and explain the controls provided by each of these techniques.
 - (a) Access to the payroll application
 - (b) Add new employee
 - (c) Employee name
 - (d) Employee number
 - (e) Employee passport number
 - (f) Basic pay
 - (g) Number of dependents
 - (h) Describe the various best practices in the data entry screen design and design a screen with radio button, check box and list box?
 - (i) What is a subsystem factory? Give an example of a subsystem factory and analyze the flow of transactions in the system?
2. You have been hired by Catalogue company to computerized its sales order entry form. Approximately 40% of the orders are received over telephone with the remainder, either mailed or faxed. The company wants the phone orders to be used as input exactly as they are received. The mail and fax orders can be batched together in groups of 30 and submitted to the computer/system. The following information is collected for each order:
 - Customer number
 - Customer name
 - Address
 - Payment method
 - Credit card number and expiry date
 - Items ordered and quantity
 - Unit price

Required

Determine the control techniques required to make sure that all orders are entered accurately into the system and discuss the differences if any, in control methods in batch and real time processing.

3. You are the manager of a model bank that has decided to install a bill payment and telephone system for its customers. The system will allow the customers to call a number to enter the system, record the bill payment transactions that they wish to make within the following 30 days, and transfer funds between savings and checking accounts. A voice feedback system will instruct the customers, on how to complete each step of the transaction. For example, 'record the date of payment and the amount to be paid'. Note: all data is to be entered using a touch-tone telephone.

Required

Because you are a senior Information System auditor of the model bank, the manager of the Information System department has asked you to advise her on the access control that you think should exist in the system. Prepare a brief report with your recommendations. Be sure to consider how the system will ensure that:

- (a) it is dealing with a valid customer.
- (b) it is allowing customers to transfer funds to or from authorized accounts only.
- (c) Customers do not overdraw from accounts.
- (d) Payments are made only to the creditors that the customer has authorized to receive such payments.

6

Network Security and Control

-
- ❖ Network—A tool for sharing resources
 - ❖ Network classification
 - ❖ Network topology
 - ❖ OSI model—A brief
 - ❖ Network cabling
 - ❖ Network devices
 - ❖ The IP network and IP addresses
 - ❖ Threats to the network
 - ❖ Controls to counter the threats
 - ❖ Technical controls
 - ❖ Perimeter security—Firewall, Router
 - ❖ Internal security—IDS
 - ❖ Management control
 - ❖ Auditing network
 - ❖ Network audit checklist
-

NETWORK—A TOOL FOR SHARING RESOURCES

Before discussing network security and the controls necessary for achieving it, we should understand the basics of what a network is. A layman's definition of a network would be, "*an intricately connected system of things*". But what does the term 'network' mean in the world of computer science? It means '*a group or system of computers that are interconnected for the purpose of sharing information and other resources, i.e. a network of computers*'. And when we say network, we do not restrict ourselves strictly to computers. Any input-output device (printers, etc.), any storage device (disk drives, etc.), can all form a part of

such a network. For example, let us say that you have a computer and your friend also has one, with a printer. Suppose both your computers are connected and made part of a network, then you can send any document from your computer to your friend's computer. Not only that, you can even send a document from your computer to your friend's printer for printing. Now, you are able to share information and other resources (computer, printer, etc.) with your friend. We can now say that your computer and your friend's computer are "networked".

Note: Henceforth, in this chapter, the terms "network" and/or "network of computers" will mean a network that consists of computers, storage devices, input-output devices, etc.

There are different types of networks that are classified based on different parameters, viz. geographical area, topology, protocol, and architecture. Though different parameters exist, the classification based on 'geographical area' is the most prevalent, owing to the ease of use of the terms and easy understanding.

NETWORK CLASSIFICATION

Based on the geographical area that a network covers, networks can be classified into the following:

Local Area Network (LAN)

A LAN is a network of computers that are geographically spread over a localized area (usually the same building). Another interesting point to note here is, in a LAN of any organization, all the components that are part of the LAN, are fully owned by the organization.

Wide Area Network (WAN)

A WAN is a network of computers that are geographically spread over a wide area (usually across cities, towns, etc.). The computers that are part of this network are usually connected by means of telephone cables, radio waves, etc. As for ownership, in the WAN of an organization, not all the components that are part of the WAN are owned by the organization. Some components, like the telephone lines, etc. are owned not by the organization, but by a third-party.

Metropolitan Area Network (MAN)

A MAN is a network that spans an entire city or town.

Note: The term MAN is not much in use at present. Only the terms LAN and WAN are used to classify any network on the basis of geographical size. The term MAN has, over a period of time, merged into the term WAN.

Apart from these, there are a couple of other networks as well:

Campus Area Network (CAN)

A CAN is a network that spans a campus (usually a University campus or a military base, etc.). It is also referred to as an Extended LAN.

Home Area Network (HAN)

A HAN is a network that is confined to the home of a user and connects all the digital devices possessed by the user.

Although the last two are not widely known and used, HAN is in much use, especially in the western part of the world, where people generally tend to have many digital devices and also “network” them for purposes of sharing and ease of use.

Based on the application architecture, the networks are classified into the following types:

Client-server Networks

In these networks, there are two different kinds of nodes (usually computers). One is a server that has very high processing power and is located in a central location. The other kind of node (client) is generally referred to as a workstation and can either have some processing power of its own or be a ‘dumb’ terminal.

There are different types of servers, viz. file server, application server, print server, etc. These networks require software, specific to servers and clients, to be installed on servers and clients respectively.

Pros

- Ease of management
- Centralized security

- Ease of backup
- Centralized resources

Cons

- Separate client-server software
- Too many clients can reduce server performance

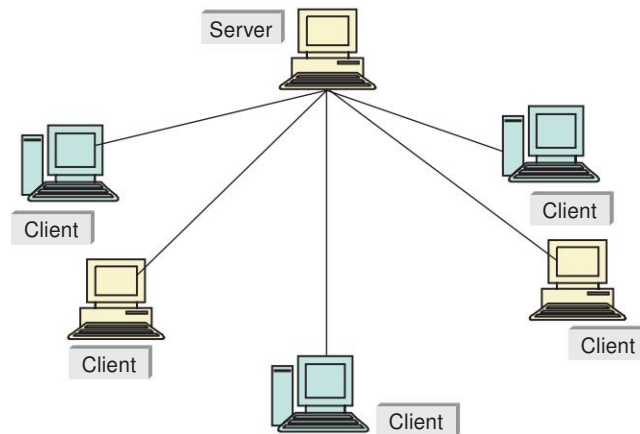


Fig. 6.1 Client-server architecture

Peer-to-Peer Networks

In these networks, each node (computer) is connected to every other node. This forms a topology, similar to mesh (as shown in Fig. 6.2). There is no such thing as a server and its client. Any node can communicate with any other node and any peripheral device (printer, etc.), connected to one node, can be accessed and utilized by any other node.

Pros

- Ease of access
- No separate software required
- Easy trouble-shooting
- High availability

Cons

- Difficult to set up
- No central security

- Difficult backup of files on the network
- Expensive and complex

This type of network is generally set up within a single room or office because of the complexity involved in connecting each node to every other node. Such kind of a network is slightly risky to manage and is therefore, used as a network for the network administrators.

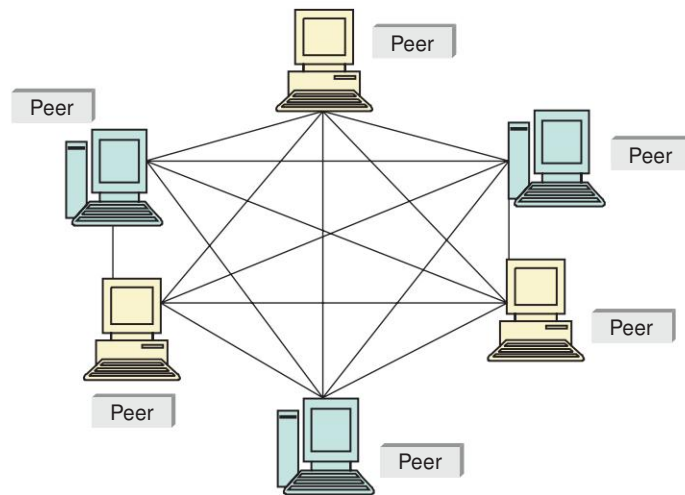


Fig. 6.2 Peer-to-peer architecture

The next section, on network topology, focuses on the other parameters, on the basis of which different networks are categorized.

NETWORK TOPOLOGY

Every network has a topology, i.e. the way that the devices in a network are arranged and the way they communicate with each other. To state a concise definition, network topology is '*the physical and logical layout of devices in a network*'. The physical structure of a network, i.e. the way that the workstations are connected to the network, through cables that actually transmit data, is called *physical topology*. The *logical topology*, in contrast, is the way that signals act in the network media, or the way data passes through the network, from one device to the next, irrespective of the physical interconnection of the devices. Though a network's logical topology is not necessarily the same as its physical topology, recent technological advances have blurred the distinctions between the physical and logical arrangements of the scattered network resources.

Since cables join these scattered computing resources together into a network, the topology of a network is also a function of the way in which the cabling is organized; whether arranged in a bus, ring or star topology— the three basic physical topologies available. All other existing topologies like hierarchical, hybrid, mesh, etc. are combinations of these three fundamental topologies. Let us now examine these three topologies.

Bus Topology

In the bus topology, all the network devices (nodes) are connected to a single, central cable called the bus or backbone. The ends of this backbone are terminated using a resistive end connector (normally referred to as a terminator) to prevent reflection and to ensure that stray signals are absorbed and not retransmitted. Ethernet is an example of bus topology.

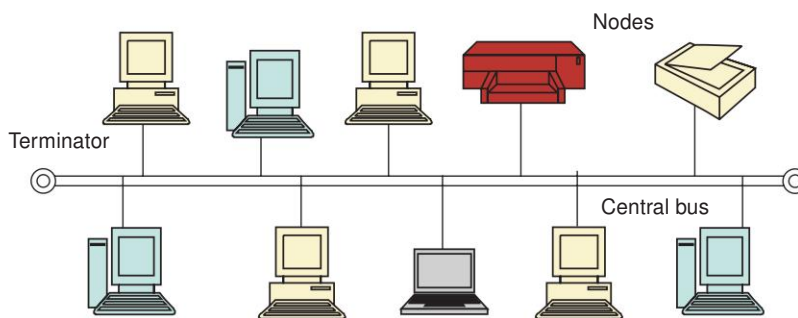


Fig. 6.3 Bus topology

All the nodes in the network share this central bus. This sharing of the transmission media (cable) has several important ramifications. Most importantly, it means that the cable can transmit only one message at a point of time, and each node on the network must be capable of knowing when it can and when it cannot transmit signals, using this shared medium.

Ethernet employs what is called a Carrier Sense Multiple Access/Collision Detection (CSMA/CD) access method to arbitrate use of the cable and to maximize its throughput. In this method, each node on the bus is always listening on the cable for transmission by other stations. It only transmits when the cable is not busy with any other transmission. It is able to sense the collision that occurs when two nodes on the bus start transmission at the same moment. Having sensed that a collision has occurred, each node waits for a random time period (usually several microseconds) before retransmitting. If a second collision occurs, the waiting period is randomly increased.

A bus topology is easy to install, but difficult to maintain and scale. Also, a fault along the bus will be difficult to locate and will affect the whole network.

The following table gives the advantages and disadvantages of a bus topology:

Table 6.1 Advantages and disadvantages of Bus topology

<i>Advantage</i>	<i>Disadvantage</i>
• Reliable for small networks, easy to use • Least amount of cable required • Easy extend.	• Difficult to trouble shoot • Heavy network traffic can slow the bus traffic.

Ring Topology

In the ring topology, the nodes are connected to one another in the shape of a closed loop, with each node directly connected to two other nodes, one on either side. Token ring is an example of ring topology.

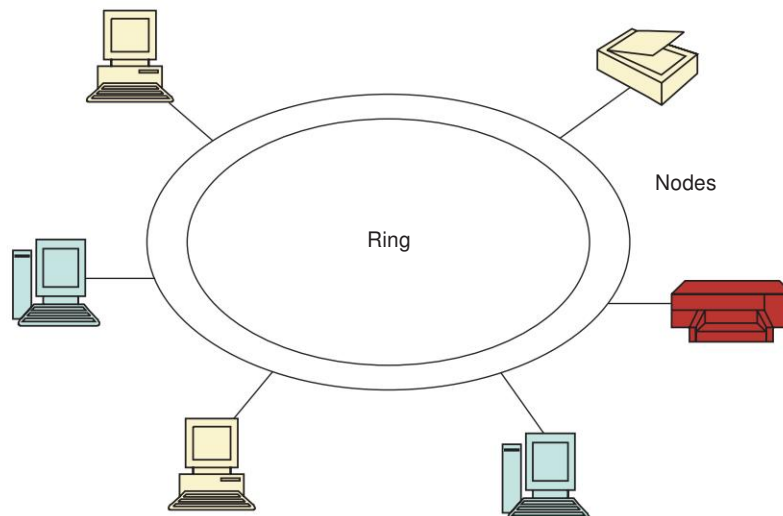


Fig. 6.4 Ring topology

In the token ring access method, an electronic signal called a token is passed from node to node on the ring, with each node regenerating the token as it is passed on. When a node wishes to transmit data over the network, it must wait until the token is passed to it by its neighbouring node. The node

takes control of the token and then places a data packet on the network. Only after the data packet has made a full circuit of the ring, returning to its originator, does the node release the token for the next workstation.

Ring topology is relatively expensive and difficult to install, but it offers high bandwidth and can span large distances.

Caution!. Token ring is a LAN technology, like ethernet and this should not be confused with ring topology. It does not necessarily mean that all networks having ring topology, will use token ring technology, they can also use ethernet technology.

The following table gives the advantages and disadvantages of a ring topology:

Table 6.2 Advantages and disadvantages of Ring topology

<i>Advantage</i>	<i>Disadvantage</i>
• High performance for a small number of workstations • Can span longer distances than other type of networks • Easily extendable	• Difficult to install and expensive • Failure of one computer can affect the whole network • Difficult to trouble shoot in case of failures • Adding or removing computers can disrupt the network

Star Topology

In the star topology, all the nodes are connected to a central device generally referred to as the hub. The hub is a common connection point for all network nodes and is generally used to connect the segments of a network together.

Alternatively, star topology could also be a network where all terminals are connected to a central processor. The star topology is ideal for Wide Area Network (WAN) applications in which outlying offices must communicate with a central office.

The principal advantage of the star topology is that it not only allows for the centralizing of key networking resources, but also gives the network administrator a focal point for network management. When something goes wrong with the network, the administrator can troubleshoot it from a single, central place.

These networks are relatively easy to install and manage, but bottlenecks can occur because all traffic must pass through the central hub. However,

these networks require that substantial investments be made in cables, because each node is connected to the central device by its own dedicated line. Also, the central hub can become the single point of failure.

The 10/100 Base-T ethernet standard permits the operation of the traditional bus-based ethernet in a star-wired configuration, using unshielded, twisted-pair wiring.

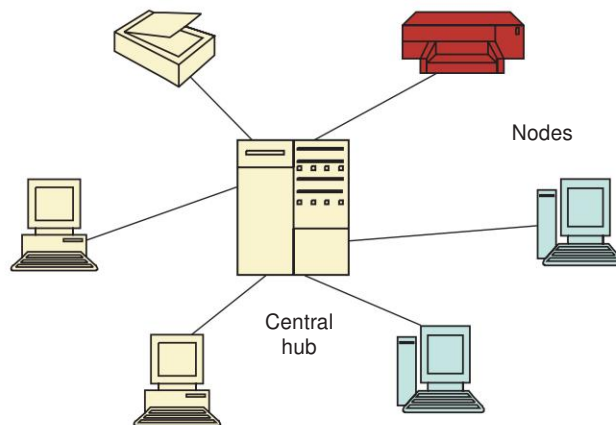


Fig. 6.5 Star topology

The following table gives the advantages and disadvantages of a star topology:

Table 6.3 Advantages and disadvantages of Star topology

<i>Advantage</i>	<i>Disadvantage</i>
• Easy to add and remove nodes • A node failure does not bring down the entire network • Easier to diagnose network problems through the central hub • Requirement of more cable	• Single point failure • Requirement for more cable

Selection Criteria for a Topology

The criteria for selection of a topology vary diversely, as per the requirements of the organization. The selection process, based on various criteria, should be able to plan and forecast the requirements, do a cost-benefit analysis of the

available alternatives, and also take into account aspects of maintenance and management of each alternative. Some of the basic criteria to be considered are the number of users, geographic location, installation, wiring, support, performance, security, cost, future expansion, and interface with other existing networks, if any. This diversity of criteria notwithstanding, certain basic features of each topology would give an indicative picture of what to choose vis-à-vis the requirements. The following table gives a picture of the features of each type of topology:

Table 6.4 Features of Bus, Ring and Star topologies

<i>Topology</i>	<i>Advantages</i>	<i>Disadvantages</i>
Bus	• High reliability • High expandability • High flexibility • Node independence	• Low scalability • Difficult fault-detection • Bus failure brings down the network
Ring	• Ease of management • Less attenuation • High bandwidth	• Expensive • Difficult installation • Node failure brings down the network • Bigger ring causes more wait time
Star	• Easy installation • Easy expansion • Centralized administration • Easy fault-identification	• Single point of failure • Lots of cable required • Traffic overload at the hub

A BRIEF LOOK AT THE OPEN SYSTEM INTERCONNECT (OSI) MODEL

The OSI model was developed as a reference model for communication. This model envisages a 7-layer architecture that forms the backbone for any type of communication between end systems. Some of the basic characteristics of the OSI model are given below:

- Layered modular approach
- Each layer performs a specific task
- Makes inter-operability simpler
- Protocols are designed around the OSI model
- Protocols establish communication between computers

The following table gives the 7-layers and their functions in brief:

Table 6.5 Layers of the OSI model and their functions

<i>Layer</i>	<i>Layer name</i>	<i>Layer function</i>
Layer 1	Physical	• Defines physical media specifications • Defines electrical specifications • Data transmission and reception to and from media • Network media— cables, copper/ fibre • Repeaters, hubs, etc.
Layer 2	Data link	• Protocol Data Unit (PDU) is bit • Interacts with the physical layer • Data framing • Error control • Flow control • Physical addressing • Bridges, Switches, NIC
Layer 3	Network	• Protocol Data Unit (PDU) is frame • Routes information, across networks • Packet fragmentation and reassembly • Routers • IP and IPX • Protocol Data Unit (PDU) is packet
Layer 4	Transport	• Adds reliability • Flow control • Error control • Message multiplexing • SPX, TCP
Layer 5	Session	• Session management • Session error control • Dialog control • Remote procedure calls (RPC)
Layer 6	Presentation	• Data formats • Data format translation • Data compression • Data encryption
Layer 7	Application	• User interface • User applications • Telnet, FTP, etc.

The following diagram is illustrative of how data flows from one node (Node A) to another (Node B)

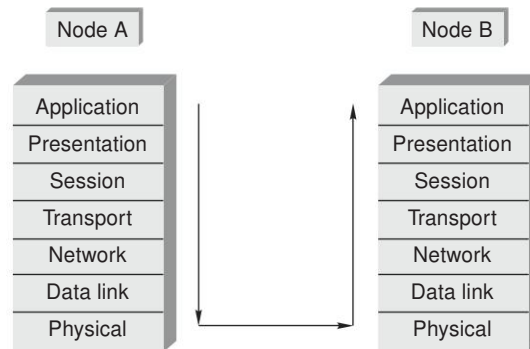


Fig. 6.6 Dataflow in OSI

NETWORK CABLING

Cables are the physical media through which all the messages are transferred from one system to another. And, just like networks have evolved, so have the types of cables that are used in connecting systems to form networks, evolved over time. Given below are some of the cable types and their characteristics:

Coaxial Cable

- Copper center shielded by a plastic insulating material.

Advantages

- Transmits up to 10 Mbps over 500 m
- Easy to install
- Low maintenance
- Good resistance to noise over long distances

Disadvantages

- Inflexible
- Low security
- Limited distance

Example

Cable TV wires

Twisted Pair Cable

- Consists of two pairs of insulated copper wires, twisted around each other.

Advantages

- Protects against cross talk and interference
- Easy to add computers to network
- Well-understood technology
- Low cost

Disadvantages

- Susceptibility to noise
- Less secure compared to optical fibre
- Distance limitations
- Requires repeating devices over longer distances

Unshielded Twisted Pair

- Pair of wires that are not shielded against electrical interference.

Advantages

- Low cost
- Easy to install

Disadvantages

- Vulnerable to electromagnetic interference and crosstalk
- Subject to attenuation (i.e. decrease in signal strength)

Shielded Twisted Pair

- An electrically-grounded, woven copper mesh, wrapped around each twisted pair.

Advantage

- Reduces Electromagnetic Interference (EMI)

Disadvantages

- Makes the wiring thick which becomes difficult to maintain
- Expensive

Optical Fibre

- Uses light, rather than voltage to indicate ones and zeros.

Advantages

- High speed transmission
- High security
- Smallest in size
- Supports voice and video data

Disadvantages

- Expensive
- Difficult to install
- Requires two cables to transmit and receive data
- Requires special connections

NETWORK DEVICES

Each network is formed not only by computers, but also certain other devices that are used to connect these computers. While there are many devices, some of which are outdated, we will take a brief look at the most basic ones. Given below are some of the devices and their characteristics:

Hub

- It is a shared medium. All systems are connected to this device through a physical crevice called *ports* on the hub
- Hub retransmits incoming signals to all outgoing lines, i.e. it broadcasts the signal

- Only one station can transmit signals at a time
- With a 10 Mbps LAN, total capacity is 10 Mbps
- Works at Layer 1 of the OSI model
- Has 1 collision domain and 1 broadcast domain

Switch

- Although a switch is also a shared medium and systems are connected to it in a similar way as they are connected to a hub, a switch has the capability to acquire some level of intelligence
- A switch gains its intelligence by maintaining a table of Media Access Control (MAC) addresses (of the systems) that are connected to each physical port
- Once it gains such intelligence, a switch can transmit messages in unicast mode and grows from a shared medium to a dedicated medium, i.e. with two pairs of lines in use, overall capacity is now 20 Mbps, i.e. $2 * 10$ Mbps
- Works on Layer 2 of OSI model
- Reduces collisions
- Has the auto-sensing feature to detect end-system speed capability
- Offers the facility to create Virtual LANs (VLANs)
- Has 1 broadcast domain and ' n ' collision domains; where n is the number of ports on the switch
- Are of two types, based on function, i.e. manageable and non-manageable
- Are of two types, based on working, i.e. store and forward, and cut-through
- Store and forward switch:
 - Accept input, buffer it briefly, then output
 - Latency
- Cut through switch:
 - Take advantage of the destination address being at the start of the frame
 - Begin repeating incoming frame onto output line, as soon as address is recognized
 - May propagate some bad frames

Router

- It is a device that is used to connect different networks
- Works in Layer 3 of OSI model
- Uses routing protocols and/or static routes to provide connectivity to different networks
- Uses “metric” to choose best path to reach the target network
- Can provide basic security at the IP level and can limit broadcast traffic
- Has n collision domains and n broadcast domains; where n is the number of interfaces on the router

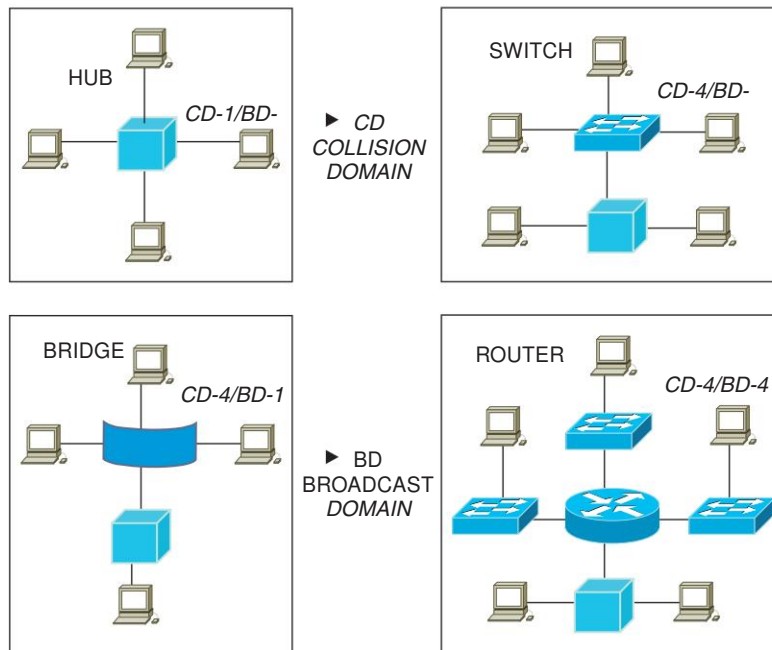


Fig. 6.7 Hub, bridge, switch, and router

THE IP NETWORK

So far we have seen the physical and logical nomenclature of the different networks. The purpose of networks is to enable sharing of information and for this, communication is essential. For communication to happen between two computers on a network or between computers on different networks,

there should be some mechanism for unique identification of a computer on a network.

When a computer is joined to a network, it is done through the means of a Network Interface Card (NIC). Each NIC has a unique address. This address is known as the Media Access Control (MAC) address. This address is also known as the Layer 2 address, since MAC is a layer 2 protocol of the 7-layer Open System Interconnect (OSI) model. This address is enough for communication between computers within a network.

For communication between computers that exist on different networks, the MAC address alone is not sufficient. In this case, we have to use an addressing mechanism that is capable of understanding the functioning of the network layer (Layer 3 of the OSI model). Here is where the Internet Protocol (IP) addressing mechanism comes into play. What is an IP address? How does this type of addressing, ensure communication?

IP Address

An IP address is one of the parts of the Internet Protocol (IP). An IP address is a 32 bit number divided into four (4) octets. It is usually written in a dotted decimal format, as shown below. It has two (2) portions which we call the network portion and the host portion. Network portion refers to that part of the IP address that indicates the network address to which that particular computer belongs. Similarly, host portion, indicates, the address of that particular computer itself, which is unique in that network.

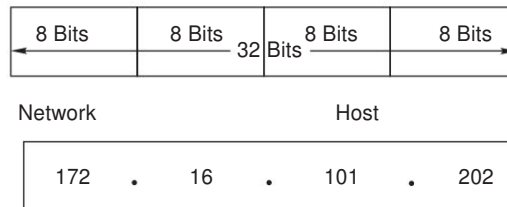


Fig. 6.8 Dotted decimal format of IP address

The number of bits in the network portion decides the “class” to which a particular IP address belongs. Let us understand what an IP address class is.

IP Address Classes

IP addresses have been categorized into different classes, based primarily on the number of bits in the network portion.

A *Class A* IP address has its first 8 bits (most significant bits), belonging to the network portion and the remaining 24 bits to the host. Also, the most significant bit in the network portion, i.e. the first bit (also referred to as the leading bit), always has a fixed value of 0 (binary 0). The other 7 bits can have one of the two binary values, i.e. 1 or 0. In other words, in a *Class A* IP address, the first octet is the network portion and the last 3 octets are the host portion.

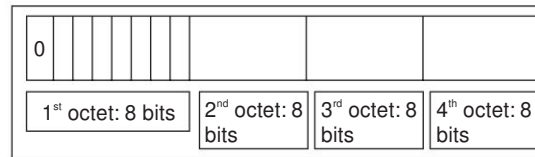


Fig. 6.9 Class A IP address

A *Class B* IP address has its first 16 bits (most significant bits) belonging to the network portion and the remaining 16 bits to the host. Also, the two most significant bits in the network portion, i.e. the first 2 bits (also referred to as the leading 2 bits) always have fixed values of 1 and 0 (binary 1 and 0). The other 14 bits can have any one of the two binary values, 1 or 0. In other words, in a *Class B* IP address, the first 2 octets are the network portion and the last 2 octets are the host portion.

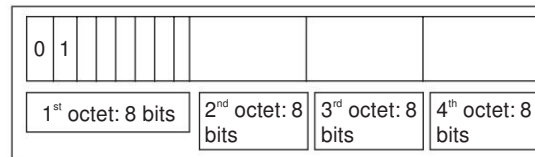


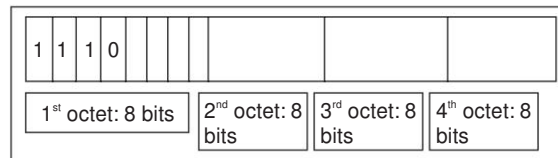
Fig. 6.10 Class B IP address

A *Class C* IP address has its first 24 bits (most significant bits) belonging to the network portion and the remaining 8 bits to the host. Also, the three most significant bits in the network portion, i.e. the first 3 bits (also referred to as the leading 3 bits) always have fixed values of 1, 1 and 0 (binary 1, 1 and 0). The other 21 bits can have any one of the two binary values, 1 or 0. In other words, in a *Class C* IP address, the first 3 octets are the network portion and the last octet is the host portion.

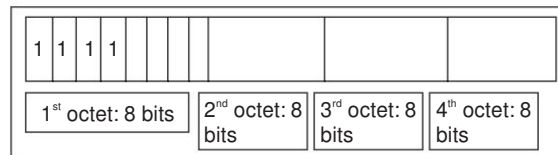
**Fig. 6.11** Class C IP address

There are two other classes of IP addresses that have certain specific functions. These are:

A *Class D* IP address is used for the purpose of multicasting. In a Class D IP address, the first 4, most significant bits, have fixed binary values of 1, 1, 1 and 0.

**Fig. 6.12** Class E IP address

The *Class E* range of IP addresses are used for research purposes by the Internet Engineering Task Force (IETF). In a Class E IP address, the first 4, most significant bits, have fixed binary values of 1, 1, 1 and 1.

**Fig. 6.13** Class E IP address

The range of IP addresses in each class, the number of networks possible in each class, the number of hosts possible in each class, etc. are given in Table 6.6.

This categorization also serves as an indicator of the size of the network of an organization, having a particular class of IP address. When an organization has such a class of IP address we say that the organization has a network of that particular class. For example, an organization using the range of IP addresses 10.0.0.0 is said to have a Class A network.

Table 6.6 The range of IP addresses

Class	Most significant bit	Number of bits in network	Number of bits in host part	Maximum number of networks	Maximum number of hosts possible in network	Range of addresses (only 1st octet)
A	0	8	24	126	1,67,77,216	1–126
B	10	16	16	16,000	65,536	128–191
C	110	24	8	2 million	256	192–223
D	1110	–	–	–	–	224–239
E	1111	–	–	–	–	240–255

Note: In the table given above, in the last column on the range of IP addresses available per class of IP addresses, the range corresponding to the IP address 127.0.0.0 is missing. Can you guess why? This is because, this class of IP address has a special functionality and is not available to be assigned to any system, on any network. The purpose of this range is to test the working functionality of the TCP/IP protocol stack on the computer. This testing is also referred to as loop-back testing.

Here's an interesting exercise. On your computer that has been loaded with the networking protocol stacks, try doing this. From the command prompt, key in the following command: *ping localhost*. What do you observe? You must get a reply from the IP address 127.0.0.1 which is nothing, but one of the IP addresses in the loop-back testing range of IP addresses.

Private IP Addresses

Out of all these classes of IP addresses, some IP address ranges have been reserved for private use. Private use includes use of these ranges within an organization, use within some closed user groups, etc. Basically, such private IP addresses cannot be used on the mother of all networks, i.e. the Internet. Therefore, if any organization uses a private IP range and still wants to get connected to the Internet, it should use some of the valid IP addresses that it can get assigned (for itself) from the worldwide body IANA (Internet Number Assigning Authority) or from any Internet Service Provider (ISP), with a presence in the area of operation of the organization. Each class of IP address has one range of IP address, reserved for private use. The following table lists the classes of IP address and their respective private ranges.

Table 6.7 Classes of IP address and their range of private IP addresses

<i>IP address class</i>	<i>Private range of IP addresses</i>
Class A	10.0.0.0 – 10.255.255.255
Class B	172.16.0.0 – 172.31.255.255
Class C	192.168.0.0 – 192.168.255.255

We will now introduce you to the terms, network IP and broadcast IP. What exactly are these IP addresses? Can they be used on any computer? Do these IP addresses have any special meaning? The next will answer all these questions.

Network IP and Broadcast IP

Network IP

An IP address having its host portion, all as binary zeroes (0) is said to be the network IP of that particular network.

For example, if 172.16.10.100 is the IP address of any computer on the network, then the network IP of this network will be 172.16.0.0. How did we arrive at this? It is very simple. Look carefully at the IP address. Can you map the IP to any particular class of IP address? Yes, you should be able to, by now. This IP address belongs to Class B. For a Class B IP address, how many bits are there in the host portion? The answer is 16, i.e. the last 2 octets. Now, if you were to make the last 2 octets have only binary zeroes, you would end up with 172.16.0.0, isn't it? Well, this is the network IP for the IP address which we had originally started with.

Broadcast IP

An IP address having its host portion, all as binary ones (1) is said to be the broadcast IP of that particular network.

Now, for the same IP address given above, what would be the broadcast IP? If your answer is 172.16.255.255, then you are absolutely on track!

Both these IP addresses cannot be used on any system, i.e. the broadcast IP and network IP cannot be physically assigned to any system on the network. The network IP is used to identify the network to which any IP address belongs, while the broadcast IP address is used for transmitting a common message/information to all the systems in that particular network.

We have seen the terms network portion and network portion of the IP address, but how exactly do we identify one portion from the other? For this purpose, there is another address, which we refer to as the *subnet mask*.

A *subnet mask* is another four octet, number similar to the IP address. Each class of IP address has a subnet mask of its own, called the *default subnet mask*. Table 6.8, given above, shows the IP address class and its associated subnet mask.

Table 6.8 IP address class and subnet mask

<i>IP address class</i>	<i>Subnet mask</i>
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

Until now we have been discussing “*classful*” IP addressing scheme. But, as with everything else that evolves, the IP addressing scheme too has grown to a state, wherein we can now talk of “*classless*” IP addressing. What does this scheme of addressing mean? It means that when we talk of any IP address, we will no longer talk of an IP address in isolation; we will instead, talk of the IP address and subnet mask, together. And we will no longer use the concept of classes to identify the network portion and the host portion of an IP address. In this scenario, given any IP address and subnet mask, by performing the binary and operation between the IP address and subnet mask, we can identify the network portion and the host portion. Also,

- Bits with a value of zero (binary zero), in the subnet mask, indicate positions ascribed to the host number
- Bits with a value of one (binary one), in the subnet mask, indicate positions ascribed to the network number

Default Gateway: It is a device that is used to forward packets from one network to another network. As the name suggests, it is usually located at the border, between two networks. This device is usually a router and has two interfaces, one interface per network. It is also possible that a default gateway may have more than two interfaces, connecting it to different networks. It can either have static routing between networks or some routing protocol that can handle routing of packets among networks.

Box 6.1**IPv6—The future Internet Protocol**

Due to recent concerns over the impending depletion of the current pool of Internet addresses and the desire to provide additional functionality for modern devices, an upgrade of the current version of the Internet Protocol (IP), called IPv4, is in the process of standardization by IETF (Internet Engineering Task Force). This new version, called IP Version 6 (IPv6), resolves some of the unanticipated IPv4 design issues and is taking the Internet into the 21st Century. IPv6 does not only allow more address spaces but is inherently more secured than its predecessor, as security in IP version 6 is considered at the design stage itself. A brief comparison between IP version 4 and IP version 6 is described below:

- **Scalability:** IPv6 has 128-bit address space, which is 4 times wider in bits in compared to IPv4's 32-bit address space.
- **Security:** IPv6 includes security in the basic spec. It includes encryption of packets (ESP: Encapsulated Security Payload) and authentication of the sender of packets (AH: Authentication Header).
- **Consideration to realtimeness:** To implement better support for real-time traffic (such as videoconference), IPv6 includes flow label in the spec. With flow label mechanism, routers can recognize to which end-to-end flow the packets belongs.
- **Plug and play:** IPv6 includes plug and play in the stand spec. It therefore must be easier for novice users to connect their machines to the network—it will be done automatically!
- **Clearer spec. and optimization:** IPv6 follows good practices of IPv4, and rejects minor flaws/obsolete items of IPv4

THREATS TO THE NETWORK

Just as everything new and evolving has a downside to it, so does the network, which has witnessed during its evolution, a proliferation of various methods of attack on itself. As more and more systems got connected to the network, the vulnerabilities inherent in those systems became to be the '*Achilles heel*' of the network. It invariably so happened, that an attack would occur only on a single system in the network, but that would be enough to bring the entire network down on its knees. In this section, we will see some of the common types of attacks on networks and a brief on how they are carried out.

- **Packet Sniffing:** This is a technique wherein, a system has its NIC in a 'promiscuous' mode and the system thus, captures all the packets

that flow through that particular network segment, irrespective of whether those packets are intended for it or not. This technique is enabled through a software called the '*sniffer*' that renders the NIC into the promiscuous mode. If you are wondering what is meant by promiscuous mode, then you should first understand the functioning of the NIC in the normal mode. In the normal mode, the NIC on a system, accepts packets that are destined only for that particular system and rejects all other packets. So, when the software renders the NIC promiscuous, it just enables the NIC, pick up a copy of all the packets, flowing through that segment. Now, once sniffing is enabled, all packets are captured and after analysis, data in the packet can be read and the user of this sniffer is now privy to such information. Such information could include usernames and passwords, account numbers, and any other type of data which can be used for malicious purposes by those with a malicious intent.

It should be noted here that to install a sniffer, you must have administrative privileges on your system.

- **Password Attacks:** In this type of an attack, a person with malicious intent tries to guess the password of a system or of another user. He/she can do this by using one or more of the following methods:
 - **Dictionary-based Attack:** Here, the attacker works on the premise that the password would be some word in the dictionary. So, all the words in a standard dictionary are tried and exhausted, until the exact match is found. This is like a hit and trial attack wherein, the person with malicious intent does not have much knowledge of the user or his/her method of working, to be able to make a safe guess of the password.
 - **Brute Force Attack:** In this type of an attack, the person with the malicious intent, tries different permutations and combinations of what he/she thinks could be the password. Brute force is used, in trying out all possible key combinations, to arrive at the password. This attack can be carried out through readymade tools that are freely available on the Internet, or can be carried out by using a combination of both, common sense and brute force, i.e. by getting some information about the intended victim, so as to zero-in on a possible password.
 - **Trojan Horse Attack:** This type of attack is trickier, compared to the other two, mentioned above. Here, the attacker tricks his/her intended victim into accepting and installing some software that masquerades as something useful for the victim,

while it actually is a tool that is intended to capture the victim's password and other details and send it to the attacker. For this type of attack to succeed, it requires the victim to be ignorant to a certain extent.

- **Social Engineering:** Here, the attacker tries to get information about the victim from the victim himself/herself or through any other source or person close to the victim. Information so gathered could include, spouse's name, children's name, vehicle name/number, house number, or any other details pertaining to the victim. This information is then used, to arrive at the password, which is generally something associated with the victim like spouse name, children's name, etc. This is a very sophisticated method of attack and requires the attacker to be very savvy and smart.
- **Network Probing/Scanning:** A probe or a scan is usually the prelude to an impending attack rather than the attack itself; a sort of reconnaissance to determine the existence of any system with vulnerabilities that can be attacked. An example of such a probe is '*port scanning*'; wherein a program or a tool is used to scan the ports that are open on a system and to try to find "suitable" ports to start an attack. Once information is gathered through scanning, other advanced types of attacks, like spoofing, etc. can then be applied to those ports that are open.
- **Account Compromise:** Traditionally, administrators continued to use factory default passwords for the 'administrator' account. Since it didn't require much effort to find out factory default passwords and the general tendency of administrators was to have simple, easy-to-remember passwords; the 'administrator' account was extremely vulnerable to compromise by unauthorized people. Also, some accounts that had the privileges of the 'administrator' account were always available on the system. This also constituted a major threat to the system and the account. Once an account is compromised, the user then has complete access to all the data and information on the system, which could then be used in a manner that the attacker wishes.
- **IP Spoofing:** This technique is sometimes also referred to as '*masquerading*'. In this method, the attacker tries to trick his/her victim by pretending to be some trusted entity, by spoofing the IP address of that trusted entity. The attacker has to first find out an entity, trusted by the victim and then find out the IP address of the

trusted entity, so as to spoof it. Once the attacker succeeds in the initial step, the victim is then under the impression that he/she is communicating with the trusted entity, which is actually not the case. The attacker then begins receiving information from the victim and this information can then be used for any purpose; malicious or otherwise.

- **Virus and Worm Attacks:** The term 'virus' is an acronym for "Vital information resource under siege". A virus is a self-replicating program that is written with the intent to initiate malicious activity on the recipient's system. A virus requires some user action, to cause it to spread to other systems. A worm is also a self-replicating program, but doesn't need any human intervention to be spread and has an effect, similar to that of a virus.
- **Man-in-the-Middle Attack:** In this type of attack, a malicious third-party, intercepts an ongoing legitimate communication between two trusted entities and then slowly begins to control the flow of communication between these entities. The malicious entity can then alter the data sent by one of the two entities, without the sender or the recipient being aware of it. This way, the attacker can trick one of the entities into disclosing confidential/secret information, by spoofing the identity of the other entity.
- **Denial-of-Service Attack (DoS Attack):** The aim of this attack, as can be guessed from the name, is not to cause theft or loss, but to render any service unusable to legitimate users of the service. It works by exhausting some resource limitation, either on the network or on the system, thereby causing the network or the system to lose its stability and stop functioning. The most common example of such an attack is exhausting the system RAM (Random Access Memory), caused by replying to thousands of 'ping' requests from a malicious user. The system is thus, not in a position to service the normal requests that it receives from legitimate users.
- **Distributed Denial-of-Service Attack (DDoS Attack):** This is one of the most difficult attacks to defend against and is an advanced version of the DoS attack. In this attack, a DoS attack is launched simultaneously, from multiple systems to target a single host or the network of a single organization.

CONTROLS TO COUNTER THE THREATS TO NETWORK SECURITY

In the previous section, we have seen some of the major threats to networks and their components. In this section, we will look at the methods by which these threats can be countered and the risks that these threats pose, mitigated. To counter any threat, there should be some kind of control mechanism that should be robust enough to allow the system to carry out its functions, irrespective of the controls imposed upon it. The controls for countering threats to network security, though mostly technical in nature, should be backed by solid administrative/management controls, so as to be effective. This section is divided into two sub-sections— one entailing the technical controls for network security and the other, listing the management aspects of the control mechanism.

Technical Controls

A network is an entity that comprises heterogeneous systems. In order to ensure security for such an entity, the control mechanism should be granular and must address all the components in the network and not be confined to just a few of them. It is apt to note here that “any network is as secure as its weakest link”. Though security is a holistic concept, controls address only specific components. Once all the controls, for all the components are in place, risk is mitigated and security is achieved. Here, it is important to remember that there is a constant trade-off between usability and controls. To achieve a fine balance between the two requires more of management skills than technical knowledge.

To achieve network security, you need to address the security at your network's perimeter, as well as inside the network. While securing the perimeter with various devices, the control mechanism will give you the required insight to ensure that the devices do what they are supposed to. The tricky part is to control your internal network. Though a few technical controls do exist for ensuring the security within your network, you will agree, as we proceed, that this area is concerned more with management and administrative than technical controls. With this introduction, let us now proceed to look at each control in detail.

Perimeter Security

The perimeter is the border that your network shares with other external networks, notably the Internet. A perimeter security system is usually the first line of defense for any organization. You can think of a perimeter security system as a sentry on guard duty, at your gate. Just as it is the duty of the sentry to check and verify the credentials of all those who enter the gate, so is the duty of the perimeter security system (sometimes referred to as the bastion host) to constantly evaluate the credentials (electronic, in this case) of all the connections that wish to pass through the perimeter, to the internal network. The bastion host not only verifies the credentials, but also has to make the decision whether to allow or deny a connection to pass through. This decision is taken, based on the policies and rules that have been configured on the bastion host, in accordance with the security policy of the organization. The security policy is a management control for ensuring security and will be discussed in the next sub-section.

Generally, a bastion host is a *firewall*. What is a firewall? A generic definition of firewall is ‘a “mechanism” that is used to protect a trusted network from an untrusted network’. This “mechanism” can either be a single system or a group of systems; can be a hardware device or a software device. There are different types of firewalls, based on their working function. Before getting into the details of the different types of firewalls, there are certain things that you should know regarding the capabilities and limitations of a firewall.

What a firewall “can” do

- Provide a focal point for monitoring of inbound and outbound network access
- Log internal-external network (usually Internet) activity efficiently
- Limit the damage that a network security problem can cause to the entire network
- Enforce a security policy

What a firewall “cannot” do

- Protect against malicious insiders
- Protect a connection that doesn’t go through the firewall
- Protect against completely new threats
- Protect against viruses, Trojans, and such variants

Types of Firewalls

There are basically two types of classifications of firewalls. One is a simple classification— hardware firewall or software firewall. Another type of classification is based on the level of functioning of the firewall— packet filtering firewall, application level firewall, and stateful inspection firewall.

Hardware Firewall

A hardware firewall is a device that is dedicated to perform the functions of a firewall. Usually, on a hardware firewall, all the firewalling functions are either “embedded” into integrated circuits or form part of a limited purpose operating system. This is done, so as to reduce the load of the firewall function on the processor. Such firewalls, whose functions are embedded into integrated circuits are also called ASIC (Application Specific Integrated Circuits) firewalls. By design, these devices generally have a higher throughput and capacity, as compared to the software firewalls. Generally, enterprises opt to choose a hardware firewall for their enterprise because of its performance capabilities.

Software Firewall

A software firewall is generally a software or program that performs the functions of the firewall and runs on a host system. It may not necessarily be a dedicated system for the firewall. It should be noted here, that the performance of the firewall is directly linked to the capacity of the host system on which the firewall is operating. Since performance is linked to the processor of the host system, a gradation of the firewall program cannot be done, as can be done on a hardware firewall. These types of firewalls are usually used in small organizations where performance or speed is not an important consideration.

Packet Filtering Firewall

- This is the simplest form of firewalls and performs simple decisions of either permitting or denying access, based on the address and port number on the packet and other rules defined by the administrator on the firewall
- Packet filtering is usually fast and most of the routers have the capability to perform packet filtering
- This type of firewall, generally works through an Access Control List (ACL), which defines the rules for permitting and denying access
- This type of firewalling is not performance-intensive

Application Level Firewall

- This is the most advanced form of firewalls and works at the application layer of the OSI model
- These firewalls are specific to applications and a firewall for one application, need not perform a similar firewalling function for another application
- It is sometimes also referred to as a Proxy server, because of the fact that it acts as an intermediary between the end-user client and the server
- Its working can be understood thus– the proxy acts as a server to the client and as a client to the server
- It does this by establishing secondary connections between itself and the server and requests the server, on behalf of the end-user, for the necessary resource
- Upon receiving the necessary resource, the proxy server sends the resource to the end-user
- The reason, this type of firewall is considered the most secure, is that a proxy never allows direct communication between the end-user and the server
- The downside of this is that, it is highly performance-intensive and has a very large memory requirement, to support the multiple connections for each user
- Another point held against the proxies is the fact that they are inflexible, i.e. new applications and protocols cannot be supported by the proxies and it takes time to develop a proxy for a new application

Stateful Inspection Firewall

- This type of firewall is the latest “generation” of firewalls
- This type of firewall works from the network layer, right upto the application layer
- Basically, this type of firewall combines some of the features of a packet filter and application level firewall to create a robust, secure, and less performance-intensive firewall
- It starts with the basic packet filter feature and drops suspect packets at the network layer itself
- It relies on algorithms to recognize and process application layer data, instead of running application-specific proxies

- It maintains the *state* of each and every packet, passing through it. *State* is the information that is derived from previous communication, if any, and other context information
- The decision to permit or deny access is thus, based on all the data available in the packet, including *state* information
- This implies that the firewall is capable of ‘remembering’ the state of each, ongoing communication passing through it, thus maintaining a high level of security
- This feature, of maintaining the *state*, enables it to scrutinize even the connectionless protocol, viz. UDP

Box 6.2**Firewalls vis-a-vis security Guard!!!**

Just imagine a security guard deployed at the entrance of your multi-storied residential complex. The duty of the security guard is to restrict the trespassers into the colony. This particular work can be done in various ways. For example, the guard should first ensure the identity of the person, the identity of the person to whom he or she wants to meet, and also the purpose of the meeting. After ensuring this, the guard tries to match it with the rule book of the tenants association, if it matches then the person is allowed entry. Such kind of work, when done by a firewall is called a “*Packet Filter Firewall*”. In such a case, the firewall checks the source (Source IP), destination (Destination IP), and the purpose (the Port number), and based on these information it matches with the rule book (Access Control List) and takes allow/not allow decision. Sometimes the tenants association decides that no outside person would be allowed a direct interaction with the tenants so the work of the security guard is to first ensure the identity of the visitor/outside person, receive the message from him/her, and communicates the message to the desired tenant. In return the security guard also carries the message from the tenant and communicates this to the concerned visitor/outside person. In such case, the security guard acts like a proxy and should understand many languages to communicate with the different kind of visitors and tenants. Such kind of work, when conducted by a firewall is called “*Application Proxy Firewall*”. In such cases, the firewall should have applications for different services like HTTP proxy, SMTP Proxy, etc. (Like the security guard should know many languages). In some other cases, the tenants association desires that the security guard should first verify the identity of the visitor/outside person and also keep a watch on the people going outside and should only allow persons to enter inside, if they have gone outside. Such kind

(Contd)

of work when done by a firewall is called *Stateful Inspection Firewall*. In such cases, the firewall will have a state table, where the particulars of the traffic going outside, are captured. The allow/not allow decision is again based on the rule book and the state table, i.e. the traffic coming inside will be checked to see whether or not it has been allowed to go outside.

ROUTER CONTROLS

The router is not only the connection point for different networks, but also acts as the first line of defense for the internal network. The points that need to be considered in the setting up and maintenance of the router are:

- *Access control list:* The access control list should be configured to:
 - Drop packets with invalid source address
 - Allow only those protocols that are required to pass through
- *Services running on the router:*
 - All unnecessary services, running on the router should be stopped
 - Do not use the default SNMP community strings
- *Configuration change and management of router:*
 - Once the initial configuration is done, changes in configuration should be done only when the working situation demands such changes
 - Only authorized personnel should be permitted to make changes to the configurations of the router
 - All the changes that are made should be in accordance with the change management policy
- *Administrative control:*
 - Only authorized personnel should have complete control of the router and its accessories like the TFTP server
 - The router should be kept in a physically secure place and should be provided with adequate protection from environmental threats like fire, etc.

Apart from the above, the points that need to be considered while configuring the router are as follows:

- Local user accounts should not be configured on the router

- The '*enable password*' on the router must be kept in a secure, encrypted form
- The router must have the '*enable password*', set to something different from the factory-enabled default password
- Drop packets that are not intended for the internal network
- The following options should be disallowed:
 - IP directed broadcasts
 - Incoming packets at the router, sourced with invalid addresses such as RFC1918 address

FIREWALL CONTROLS

The following points need to be considered when opting for a firewall:

- The firewall should work in the mode, in which it blocks all the traffic, except those specified, for the purpose of easier manageability
- The firewall should have proper fail-over and redundancy
- The firewall should have scalability
- The firewall should be able to handle the network throughput, without affecting the performance of the network
- There should be a proper mechanism for updates/patches to be applied to the firewall
- The configuration of the firewall should be done by authorized personnel
- The firewall should be configured to allow only those protocols that are required
- The Access Control Lists (ACLs) on the firewall, should be created as per the requirement, and the flow of traffic should be enforced according to the ACLs
- The firewall should have a logging mechanism that can be customized to suit different needs
- The alerting system of the firewall should be monitored periodically for alerts
- Any change in the configuration of the firewall, should be made only when required and should be in accordance with the change management policy
- The original firewall configuration and any changes thereto, must be reviewed and approved by the appropriate authority

These perimeter security controls should be driven by proper management controls, so as to be effective. It should be noted, that even the best firewall will fail to protect a network, if it is not administered properly and consistently. The management controls for the perimeter controls are given in the next sub-section.

INTERNAL SECURITY

This is the most vital part of securing an organization's network. You may have noticed that most of the Internet surveys, conducted to probe the patterns of breach of network security, have concluded that 75 per cent of detected and reported attacks and purported attacks, originate from the internal network of an organization. Though this figure is staggering, it is not hard to believe this statistic because of the fact that people in the internal network who have more access to information and knowledge about the entire network and its components than external users. More importantly, people on the internal network have a greater chance of knowing the loopholes and lacunae in the network, which significantly increases their potential to cause risk. It is of paramount importance therefore, to ensure security in the internal network to ensure total security for the network of the organization.

In the internal network, controls should be more of a monitoring and detective nature than protective. One of the major controls for monitoring the internal network is the Intrusion Detection System (IDS).

IDS

An IDS is a monitoring and detecting system that has the capability of alerting the administrator of the network (or system), of an impending attack. There are different types and classifications of IDS.

IDS can be classified as either, *Host-based IDS (HIDS)* or *Network-based IDS (NIDS)*. As is evident from the names, HIDS monitors a single host, while a NIDS monitors an entire network or an important segment of a network.

Based on their working, IDS can be classified as either, signature-based IDS or behaviour-based IDS.

Signature-based IDS

This type of IDS, works by matching the pattern of each and every packet, with a pre-defined database of signatures, pertaining to malicious activity. This type of IDS is similar to the present-day antivirus.

Behavior-based IDS

This is a much more complicated system. This type of IDS works by first, profiling what the administrator (or the user) terms as *normal* activity. This is a kind of learning process for the IDS and once an understanding of *normal* activity has been acquired, the IDS can be deployed. Once deployed, all activity on the system is then compared against its *learned* database of *normal* activity. If the IDS finds any deviation in the activity from the *normal*, it takes suitable action that it has been programmed to perform. It is pertinent to note here that this type of IDS is slowly gaining popularity and acceptance, and this area is still fertile for research.

IDS Controls

Any IDS should necessarily have the following:

- The ability to react in time, to prevent substantive damage, by automatic or manual intervention
- The ability to identify the precursor of the more serious attacks
- The ability to identify the perpetrator of the attack
- The ability to discover new attack patterns
- The ability to produce evidence

Apart from the facilities provided by IDS, mentioned above, the following need to be considered when implementing an IDS:

- Use a respected commercial package that is regularly updated to keep abreast of new vulnerabilities and attacks
- Keep the intrusion detection tool up-to-date, by applying the latest patches and attack signatures
- Run the absolute minimum services on the platform, hosting the intrusion detection tool
- Do not allow the platform's interface to become visible to the perimeter networks being monitored
- Establish an administration and reporting network for the intrusion detection system and isolate it from the internal network
- Do not rely extensively too much reliance on the intrusion detection tool and ensure that other security procedures are in place

Management Controls

Security means different things to different people. To a system administrator, it might mean making sure that servers are hardened; to a network administrator, deploying the right firewalls and Intrusion Detection Systems. To a developer, writing a few lines of codes, using SSL, etc. and to the CEO it means that the business is reasonably protected from loss. The CIO's (Chief Information Officer) perception of security, lies somewhere in between these extremes, as he/she is worried not only about the technical aspects of security, but also such issues as customer's privacy, security audit, and configuration management of system and software. Different levels of responsibility, functions, and perceptions, may sometimes lead the people of an organization, to have an unsympathetic attitude towards each other. So, while the system administrators do not agree with the importance accorded to policy and procedures, the internal auditor does not care about the technicalities involved in implementing the policies and procedures. So what is the solution? The solution is management control and support. Such control keeps all other controls together and makes the system resilient. Management control for network operations, essentially envisages, planning for the network, framing the network security policy and procedures, establishing the management framework with roles and responsibilities of different personnel who are associated with the network operation, and finally, the top management's support to the overall information security/assurance program for the organization.

AUDITING NETWORK

Network audit is a very broad area and its scope is dependent on the respective audit charter or engagement letter. A comprehensive network audit should determine the effects that a malfunction of a network component might have on the system, the user, the application, and most importantly, on the business itself. Controls, to ensure proper security performance and reliability of all network components, must be assessed during the audit. Accordingly, the following considerations should be addressed during a network audit:

- Is the network cost-effective? Are its operation and design, consistent with the project system development lifecycle?
- Is physical security sufficient, to safeguard equipment and information, as well as the personnel operating or using the system?
- Is critical data being protected from loss or damage?
- Is sensitive data being protected from unauthorized exposure?

- Is the management providing the appropriate direction, policies, and standards for effective network computing service?
- Is compliance with established policies and standards being monitored regularly?
- Are appropriate hardware and software techniques being used, to ensure network reliability?
- Are controls sufficient to ensure that access to the network is limited to authorized users?
- Are network utilities and management programs being controlled properly?
- Does the system meet user requirements?
- Are facilities available, to measure performance?
- Is there a methodology in place, to ensure sufficient resources (capacity planning)?
- Are there any operational procedures to ensure that critical system functions are available?
- Does the network design, afford sufficient flexibility and resilience, to limit disruption?
- Does a backup mechanism exist, in case of media failure?
- Is there a business-related, contingency backup plan, or is the network included in a larger plan?
- Is there any methodology for enforcing policy guidelines?

A comprehensive network audit for an organization, like a bank which has opted for a core banking solution, with multiple delivery channels like Internet Banking, ATM, etc. would include the following steps:

Cataloguing the Network

In order to give their views on the security and control aspects of the network, auditors need to know the various components of the network and how they are assembled. For knowing about the various components, the first and foremost requirement is the network catalog. The various components of the network catalog are:

Network Drawing and Diagram

This map of the network will provide an overview of the entire network. The auditor should get this map from the network manager.

A Form Identifying Servers within the Wide Area Network

This form should list the various servers in the network. The other information which the form should include is network segment (name of the network segment which contains this host), Host name, Host IP address, the subnet mask (which could be common for many hosts), the computer type (make of the computer), and the operating system.

Catalog of Communication Services and Circuits

This will include the various types of services within the network, the circuits used, and the speed of the circuits. The information that is required to be catalogued includes, the name of the supplier (carrier name for the circuit), the circuit media (for example, coaxial, fiber optic, etc.), the circuit type (*E1*, *E2*, *T1*, *T2*, etc.), the origination point of the circuit, the termination point of the circuit, and the circuit speed (64 kbps, 2 mbps, etc.).

Catalog the Data Switching Equipment

This form will contain particulars (the identification features) of all the hubs, bridges, and all other gateways. The particulars to be included in this form are equipment type (hub, bridge, switch, router, etc.), the IP address, the inbound address (the address that can send inbound transmission to the network), the outbound address (the address that can send outbound transmission to the network), the physical location, etc.

Router Tables

This form will contain, the network segment, the device type (router, layer 3 switch, etc.), the network address, and the reference number of the places or the page number where the router table is printed.

Firewall Particulars

Like the router table form, this form should also contain the name of the network segment, the device type (make of the firewall), network address, and the pointer for the firewall configuration.

Identifications of Workstations within the WAN

The particulars of the hosts, workstations connected to the WAN/LAN, viz. network segment, user name, the IP address, the type of computer, the

identification of the hub/switch to which it is attached, and the primary function, should be part of this form.

Identification of Connection to Internet and Other Public Network

This form should contain, the name of the ISP, the public IP of the router where the link terminates, the IP address of the firewall through which the traffic enters the private network, etc.

Trading Partners Connection

This form will contain particulars to help identify the trading partners that connect to the network and will also provide additional information about the trading partner, viz. the interface address, the purpose, etc.

In a proper network environment, the cataloguing of the network is an ongoing exercise and the auditors will have to customize the data as per their requirement. In environments/organizations where it is difficult to find proper network cataloguing, the auditors should not spend their auditing time in preparing the catalog. In stead they should advise the client on how to prepare the catalog, as per their specifications, before the commencement of audit. This will help save precious audit time.

Auditing Network Architecture

Once the cataloguing is over, the auditor should access the network architecture to understand the overall requirements of the network and to identify its weaknesses. The study areas that need to be covered in this step, include:

The Network Topology and the Redundancy

This will include studying the network topology and finding out its efficacy and areas of redundancy.

The Logical Access Control and Trust Level

This will include studying the various zones/subnets of the network and evaluating the logical access control and the trust level. This step can also help evaluate the adequacy of components in various zones.

High Availability and Single Point of Failure

At this step, the auditor should assess the availability of the required infrastructure and the single point of failure. The single point of failure is very important from the organization's point of view, as the failure of this component will jeopardize the entire network.

Vulnerability Assessment

After the security analysis of the architecture is done, the auditor should conduct the vulnerability assessment of the servers, firewall, and network devices. The assessment will comprise running customized scripts to obtain the relevant system information, and validating the results of the script output by manual verification. The detailed, component-specific report should be kept as evidence. Such vulnerability assessment, for gateways and other equipment, having a public IP interface, can be done remotely, through the Internet.

The vulnerabilities found thereupon can then be classified into three categories, viz. system vulnerabilities, insecure settings and unnecessary services.

System Vulnerabilities are weakness in the OS or application software, running on the server. An attacker may exploit these vulnerabilities for two purposes:

1. To gain privileges and access to the servers
2. Carry out denial-of-service attacks and prevent legitimate users from accessing the services provided by the servers

Insecure Settings are generally, the default installation of OS/IOS, which come with a number of unsafe settings that can be exploited by malicious users or attackers. A hardening procedure should be applied on these components/servers, to remove these insecure settings.

Unnecessary Services are some extra services, which could be innocuous, may be running in the servers, and other components. Such services consume the valuable resources on the servers, and sometimes provide additional opportunities for the attacker.

Process Audit

After the vulnerability analysis the auditor should start conducting the process audit of the infrastructure. The process audit, checks compliance of network practices with the defined policies and procedures of the organization/bank. As part of the process audit, the existing practices will be benchmarked against

the best practices in a banking environment and the adequacy of the policies and procedure will be analyzed. The various components of the process audit are as follows:

Evaluating the Procedures

The auditors should ensure that:

- Procedures are clearly defined as per the bank's specific requirements and environment
- Procedures must be independent of people
- Procedures should be capable of projecting lapses and instances of non-compliance
- There is accountability for the lapses and non-compliance
- Procedures must be self-correcting

Asset Classification and Ownership

Some of the important issues regarding asset classification, which auditors should assess are the classification and ownership of assets which must be distributed, based on the amount of time that the personnel can commit to the resources in question. It should not happen that all the assets are owned by senior-level personnel who can hardly devote time to the assets. Sufficient skill-levels must be developed internally, to understand the risks and implications of the activities that are performed.

Roles, Responsibilities and Control Structure

In this step, the auditor should look at the roles and responsibilities of key functionaries like the Chief Information Security officer and network administrator and also find out the role conflict and the control structure, viz. the separation of duties, etc. At this stage, the auditors should also observe the minutes of various management committee meetings to see whether the issues are appropriately discussed in the management forums or not.

Router/Switch/Firewall/IDS Management Process

Proper documentation of all these devices should be maintained at a central place, with a backup, at a different place. Such documentation should contain details of access rights and the purpose and period for which these have been permitted. While reviewing these documents, the auditors should ensure that they are reviewing the appropriate document (not the one which has been made exclusively for the auditor).

Antivirus Process

The auditor should ensure that all the systems, connected with the network, should be updated with the latest antivirus software. In case of a core banking environment, this should be done at the gateway level and pushed to various segments, across the enterprise. The automated process should:

- Check the appropriate vendor sites for the release of antivirus software
- Download the updates, using an isolated machine, connected to the Internet
- Move the signatures to the servers and workstations, in the Network Operating Center (NOC/ datacenter) and branches
- Update the antivirus software with the new signatures

As far as possible, this entire process should be automated, as the manual process is person- dependant and time consuming, whereas a serious virus attack would be fast and destructive.

Backup Procedures

At this point the auditor should evaluate the documented backup policy and procedures and find out their efficacy. Online backup or more frequent backups for sensitive servers, viz. the database server in a core banking environment, must be considered, to help reduce the loss of data that can occur due to failure of the server.

Incident Handling Procedures

Incident handling is an important aspect of any secure environment. Some examples of security incidents are accidental removal of critical data by the administrator, unauthorized access to the server by a person with malicious intent, an antivirus attack, etc. It is important to have proper identification of incidents and this requires incident handling procedures. The action that needs to be taken after an incident, also needs to be clearly documented, so that the administrator's actions do not inadvertently remove critical information that would be useful in finding the source of the attack. The awareness of the IS/ network personnel about incidents and their response to these is very important for efficient implementation of the incident response policy and procedures.

Log Monitoring Procedures

Events and logs, generated by the various components, viz. servers, router, firewall, IDS, and applications, are major sources of information about errors

and suspicious activities. It is imperative that the logs be checked and analyzed on a regular basis. The problem in log analysis is the huge amount of log that is generated by different devices. If not parsed and managed properly, the sheer size of the log itself, will become the reason for the malfunctioning of various components. It is always better to acquire automated log parsers, identify a server for log aggregation and enable the auditing facilities, available for various operating systems, for an effective collection and evaluation of various logs.

Patch Management Procedures

The patches and hot-fixes, affecting the servers and applications, need to be tracked closely and the system must be patched up using the latest patches, released by different vendors. Considering the number of frequent patches released by various vendors, it is always advisable to have proper patch management procedures. Now, there are tools available, which will help in centralized patch management for both, the operating system and applications. The responsibility of tracking system vulnerabilities must also be assigned. When system vulnerabilities are notified and patches are released, they must be tested to verify that the patches are not affecting the functioning of the application and only then applied on to the servers.

Administrative and Desktop Practices

A “clean desktop” policy should be followed, to avoid access to information by unauthorized personnel. Groups that have been assigned different administrative roles, must be created on the servers and user accounts should be created and added to the groups. The user accounts must be different for different administrators and the passwords should not be shared.

Change Management Procedures

The auditor should assess the change management procedures of the network operation to ensure that all the changes in the configurations and settings are documented and as per procedures. For ensuring this, a sample configuration file may be taken, and the particulars may be checked for valid approval.

Different audit procedures are followed for giving an opinion about the effectiveness and efficiency of the processes involved in the network operation. These could include interviewing key personnel, observing the processes and evaluating various policy and procedure documents.

A SAMPLE CHECKLIST FOR NETWORK AUDIT

I. Service provider checklist

Questions	Yes/No	Remarks
Are multiple service providers, available in your areas of operation? Sometimes it is required for sensitive applications like Internet banking. 1. If available, is more than one service provider used for sensitive applications? 2. Are formal Requests For Proposals (RFPs) issued? 3. Are sealed tender bids used? 4. Are the tenders evaluated fairly? 5. Are selection criteria and the processes documented? 6. Is the network accessible through multiple central offices? (The two service providers may be operating from the same exchange; so the risk is not significantly reduced.) 7. Is there a business continuity plan for the network service providers? Also: (a) Has it been tested? (b) Is it current?		
II. Network contract checklist 1. Was a special contract like the Service Level Agreement (SLA) drawn up for each network service provider? 2. Are the responsibilities of the service provider clearly defined? 3. Have installation dates been specified? Have the following also been specified? (a) Time frame (b) Penalties for missing specified data (c) Remedies in case of delay 4. Have installation costs been clearly identified? Do these include: (a) Equipment cost (b) Labour cost (c) Travel cost 5. Have acceptance criteria been specified in the SLA? If yes, has this been done: (a) In sufficient detail?		

(Contd)

Questions	Yes/No	Remarks
(b) With minimum level of performance guaranteed? 6. Have performance standards been clearly established? 7. Has the tariff structure been appended to the SLA? 8. Does the vendor have the freedom to change the tariff structure for the duration of the SLA? 9. Are payment terms and conditions specified in the SLA? (a) Are these terms consistent with the organizational policy? 10. Are there any remedies in case of non-compliance with the performance clause? Does the clause include: (a) Definition(s) of 'non-compliance with performance'? (b) Remedies for each type of non-compliance with performance? (c) Compensation for lost time and material? (d) Protection measures, to ensure that the organization is held safe from liability, in the event that the service provider does not perform as per the SLA? 11. Is there any recourse in the event of breach of SLA? 12. Are the detailed system specifications included in the SLA? 13. Is there a multi-vendor responsibility clause? 14. Are service levels clearly identified and guaranteed? 15. Are the maintenance and service costs specified? (a) Have these been specified for the term of the SLA? (b) Are the rates fixed? (c) Do the rates vary according to the working hours? (d) Are the rates inclusive of travel costs, if travel is required to be undertaken? 16. Are problem reporting procedures specified? Within these: (a) Is there a mention of the response time? (b) Are escalation procedures specified and agreed upon? 17. Are there provisions to minimize the impact of network failure? Also, are there provisions for: (a) Alternative service providers?		

(Contd)

Questions	Yes/No	Remarks
(b) Multiple grids? (c) Multiple central offices (exchanges)? 18. Does the service provider have a disaster preparedness plan ready for installation? (a) Is it up-to-date? (b) Has it been tested? 19. Are there any warranties in the SLA? (a) Has anything been excluded from these? (b) Are there any limitations? 20. Is a statement of the service provider's expertise included in the SLA? 21. Was the legal department involved in formulation of the SLA, before the signing of the SLA?		
III. Checklist for dialup lines		
1. Are dialup lines clearly identified? 2. Are phone numbers unlisted? Are these: (a) Restricted to authorized individuals? (b) Capable of being changed on transfer/termination? 3. Is dialup access allowed on a need basis? 4. Is dialup access restricted, based on the rule of least access? (a) By application? (b) By transaction? 5. Have phone numbers been removed from handouts? 6. Are users identified and authenticated? What is the mechanism used? (a) Passwords? (b) MAC (media access control) codes? (c) Secondary authentication techniques? (d) RADIUS? (e) TACACS? 7. Are passwords and MAC codes changed on a regular basis? 8. Is dialup usage monitored? Is monitoring done: (a) By the user? (b) Byline?		

(Contd)

Questions	Yes/No	Remarks
9. Are caller identification services used (where available)? 10. Are only authorized locations listed for dialup use? 11. Are call-back techniques in place, to ensure that the user is calling from an authorized location? 12. Is dialup control software in use (defender II, etc.)? 13. When lines are not in use, are the modems disabled? (a) Are modems used for backup of failed leased lines? 14. Are error detection and correction techniques in use? 15. Are encryption or scrambling devices used wherever appropriate? 16. Are dialup circuits subjected to a periodic, requirement analysis? 17. Is demon dialer used on a regular basis to identify unauthorized modems? 18. Have all modems been consolidated into a modem pool? (a) Is secondary authentication (secure ID cards, etc.) used on inbound lines? 19. Are all modems disconnected when not required? IV. Checklist for leased circuits 1. Are circuits adequately concealed and protected? 2. Is access to the telephone room restricted? 3. Are data circuits separated from voice circuits (wherever feasible)? 4. Are circuit monitors used to detect unauthorized taps? 5. Are volumes monitored? If yes, are they monitored: (a) By application? (b) By user? (c) By circuit? 6. Are errors monitored? (a) Are detection techniques in place? (b) Is problem reporting information logged? (c) Has meantime between failures been calculated? (d) Service provider response time? (i) Initial response time? (ii) Time to repair? 7. Are backup circuits available for critical applications?		

(Contd)

Questions	Yes/No	Remarks
8. Are alternate paths available to critical DTEs? 9. Where there are multiple, low-speed circuit link sites, has line consolidation been considered? 10. Is encryption used (where applicable)? 11. Are service personnel authorized, and accompanied by authorized in-house personnel? 12. Are periodic inspections made to detect patches? (a) Is identification of patches done? (b) Is justification for use of patches, done? 13. Is test equipment used only by appropriate personnel? 14. Are problem reporting procedures in place? Are these: (a) Reviewed by the management? 15. Are lines monitored for errors? For this, is: (a) Line conditioning used? 16. Are periodic checks made with the service provider to determine if circuits have been digitized?		
V. Checklist for coaxial cable 1. Are all circuits clearly identified? 2. Is there an up-to-date circuit map, detailing where the cables are strung? 3. Is all wiring concealed? 4. Are cables periodically scanned for taps? 5. Are lines monitored for errors? 6. Are all wiring closets (or panels) locked? (a) Are accesses controlled? (b) Are accesses logged? (c) Is there dual custody where appropriate? 7. Have unused lines been detected? Also, have these been: (a) Removed? (b) Disconnected from the controller? 8. Do critical terminals have an alternative path? 9. Are installers and service personnel closely monitored? 10. Are periodic inspections of data terminal equipment made for unauthorized splitters? 11. Are lines monitored for over/underutilized circuits?		
VI. Checklist for fibre optic 1. Are all conduits secured?		

(Contd)

Questions	Yes/No	Remarks
2. Are there up-to-date circuit maps? 3. Do critical DTE's (Data Terminal Equipments) have alternative circuit capability? 4. Are service personnel authenticated and monitored? 5. Are statistics maintained and reported to the management? (a) Statistics on errors (b) Statistics on failures (c) Statistics on time to repair VII. Checklist for microwave 1. Are microwave communications mentioned in service provider contracts? 2. Is confidential data encrypted, prior to transmission over microwave circuits and channels? 3. Are error rates monitored by the circuit? 4. Are statistics and problem logs maintained? 5. Are backup circuits available for critical data terminal equipment? VIII. Checklist for satellites 1. Are satellite circuits in use? 2. Was a cost justification, performed for satellite services? 3. Have sensitive data transmissions been identified? 4. Is encryption used for sensitive transmissions? 5. Are procedures to detect unauthorized deletion/insertion of messages in place? 6. Are circuits monitored for (a) Error ratio? (b) Lost messages? (c) Circuit failures? (d) MTBF (Mean Time Between Failures)? 7. Are ground stations and facilities secured? 8. Are backup circuits available, in case of satellite service disruption? 9. Are data volumes monitored? Is this done: (a) By the user? (b) By the circuit?		

(Contd)

Questions	Yes/No	Remarks
10. Are underutilized circuits used for other purposes like? (a) Voice communication (b) Video conferencing IX. Checklist for packet-switching, frame relay and ATM 1. Are international standard packets, frames and cells used? 2. Are all points of access to the service provider's nodes, secured? 3. Is message sequencing used and monitored? 4. Are site addresses private (not published)? 5. Are packet, frame and cell volumes monitored? Is this done: (a) By the user? (b) By site? (c) Point-to-point? 6. Is the service provider providing detailed usage information in an electronic form? 7. Are unusual volume changes monitored? And if noticed, are these: (a) Investigated? 8. Are error-detection, resolution and reporting techniques, in place? 9. Is packet switching, frame relay or ATM used for disaster preparedness and business continuance? (a) Has it been tested? (b) Has this been done recently? 10. Are packets, frames and cells, encrypted? X. Checklist for public networks 1. Does the organization have Internet or other public network access? 2. Does the organization have a registered domain name and an IP address? 3. Is there a policy for public network access? (a) Is access distributed to all networked employees? (b) Has the policy been enforced? (c) Does it include the do's and don'ts of safe usage? (d) Has the risk of unsafe usage been highlighted?		

(Contd)

Questions	Yes/No	Remarks
(e) Are all procedures described in an easy-to-understand format? (f) Are users aware that their public network activities may be monitored? (g) Are users informed of the penalties for failure to comply with safe usage procedures?		
4. Is public network usage training, provided to all users?		
(a) Does the training provide examples of safe usage?		
(b) Are the benefits of using public networks highlighted?		
5. Are there procedures in place, to monitor the usage of the public network and enforce safe computing practices?		
6. Are firewalls set up between the corporate network and the public network to isolate corporate information resources from the public network?		
(a) Are the access lists documented and reviewed?		
(b) Is unusual activity investigated promptly?		
7. Is there an account of the amount of traffic flowing from/to the public network?		
8. Have all machines that connect to the public network, been hardened for network and system security?		
9. Is there a 'trespassing' notice on the login screen, to deter any casual attempt at entry?		
10. Are the firewall logs reviewed to identify:		
(a) Visits to undesirable sites?		
(b) Excessive usage by employees?		
(c) Attacks on the firewall from the Internet?		
11. Has the web server been properly secured?		
(a) Is it isolated from the rest of the network?		
(b) Is the web page code secured?		
(c) Is port 80 and/or 443, the only port open?		
(d) Are site statistics maintained?		
12. Is encryption used for sensitive transmissions?		
13. Is the Internet connection penetration, tested on a regular, surprise basis?		
(a) Is an outside penetration team used for this purpose?		
14. Is the security of the ISP, tested on a regular basis to ensure that they:		

(Contd)

Questions	Yes/No	Remarks
(a) Are secure? (b) Provide the services they agreed to perform? (c) Have been audited? 15. Are the Internet and security staff, reviewing CERT bulletins daily? 16. Are all appropriate security patches applied regularly? XI. Checklist for network connectivity devices 1. Have all network connectivity devices been identified? 2. Have all security features been implemented, on each of the network devices? (a) Have security features been catalogued by devices? (b) Are the security options reviewed periodically, to determine if other options should be selected? (c) Are the vendor's security enhancements downloaded, tested and implemented on a timely basis? 3. Have vendor default passwords been changed? (a) Are the passwords complex? (b) Are they changed on a regular basis? (c) Are they changed when services of the network staff or contractors are terminated or when they leave voluntarily? (d) Are the passwords changed after vendor troubleshooting? 4. Are the direct-dial modems that are attached to any of the network devices, disabled when not in use? 5. Do vendors have remote access to routers? (a) If so, is their access monitored? (b) Are vendor changes, subject to your organization's change management procedures? 6. Is accounting used on routers or firewalls? (a) Is unusual activity investigated? (b) Are unknown addresses investigated and resolved? (c) Are changes documented? (d) Are differences investigated? 7. Are router, firewall, hub and switch configurations catalogued? (a) Are they stored in a safe manner? (b) Are the files read and write-protected?		

(Contd)

Questions	Yes/No	Remarks
(c) Are they stored off-line, on removable media? 8. Are hacker penetration attempts investigated? (a) Are there strong practices in place, to identify the point of penetration and any files the hackers may have placed on the network? (b) Are there mechanisms to identify any back doors that may have been installed by the hackers? (c) Are penetration attempts monitored, tracked, and reported to the management? (d) Are criminal or civil actions taken against hackers who attempt to penetrate or have successfully penetrated the network? 9. Are access control lists for routers and firewalls examined regularly, to ensure that they continue to act as effective controls? 10. Is a firewall or proxy server used to protect the Internet connection: (a) Has it been penetration-tested? 11. Are internal modems used to bypass the firewall/proxy server and go directly to an ISP? 12. Are workstations with modems identified? (a) Is the need for a modem for that user justified? (b) In such a case, is that system disconnected from the network? 13. Are procedures in place, to identify users who are by passing the firewall to get to the Internet? 14. Is Internet intrusion-detection software used, to detect intruders? (a) Is the output reviewed? (b) Are there automated alerts when a penetration is detected? (c) Is action initiated, based on the alerts? (d) Are the actions automated or manual? 15. Are vendors permitted to access the router and firewalls, remotely? (a) Are there authentication procedures in place, to verify that they are in fact authorized vendors? (b) Are manual procedures in place, to authenticate the vendor?		

(Contd)

Questions	Yes/No	Remarks
16. Are network management software and devices in place, for monitoring and maintenance?		
XII. Control checklists		
1. Is there a security policy for all networks that connect to the network?		
2. Does the security policy include the following items:		
(a) Intruder detection?		
(b) Reporting?		
(c) Pre-emptive security?		
3. Is the management aware of the risks associated with interconnected networks?		
(a) Is network security adequately funded in all respects?		
4. Is there a chief security officer and does he/she report to the senior management?		
5. Do the security officers have the skills, required to install and maintain security on all platforms?		
6. Are there formal procedures in place, to detect penetration attempts?		
XIII. Checklist for network disaster preparedness		
1. Is there a comprehensive, tested disaster plan?		
2. Have all preventive, containment measures been addressed?		
3. Is there at least 25 per cent surplus capacity to enable switching around failing critical circuits?		
4. Is there a connection to a secondary WAN, for critical applications?		
5. Are there strong testing procedures for:		
(a) Hardware?		
(b) Software?		
(c) Network components?		
6. Is the network properly documented? Is it:		
(a) Current?		
(b) Easy to understand?		
7. Are key network staff members, cross-trained?		
(a) Do key employees have backups?		
8. Is the plan updated regularly, to reflect changes?		

(Contd)

Questions	Yes/No	Remarks
9. Is there a network disaster coordinator?		
XIV. Checklist for auditing network operations		
1. Is the Network Operations Centre (NOC) secure?		
(a) Physical access?		
(b) Hazards?		
2. Is access to the NOC, restricted to network analysts?		
3. Are network monitors use:		
(a) To monitor the network, proactively?		
(b) To respond to client complaints?		
4. Are hard copy logs, in use, to record analyst sessions?		
5. Is access to the network monitor, strictly controlled?		
6. Are monitor IDs non-standardized (i.e. difficult to guess)?		
7. Are network analysts supervised?		
8. Are operational objectives and reasonable service levels specified?		
9. Upon report or discovery of a problem, are incident reports initiated and forwarded?		
10. Are network analysts trained on a periodic basis?		
XV. Checklist for network management		
1. Is the senior-level management actively involved in network management? Also, does it:		
(a) Demonstrate commitment?		
(b) Support network management activities?		
2. Is the management aware of the complexity of the network management function?		
3. Is the management aware of the need for security?		
4. Have service levels been developed? Are these:		
(a) Reasonable?		
(b) Approved by the management?		
(c) Reviewed periodically?		
5. Does the management receive regular network reports?		
(a) Performance?		
(b) Service level exceptions?		
(c) Unusual situations?		
(d) Proposed service enhancements?		

(Contd)

Questions	Yes/No	Remarks
6. Is the management aware of the cost/performance of various service provider alternatives? (a) Satellite? (b) Leased circuits? 7. Is the management aware of the security implications of the service provider alternatives? XVI. Checklist for auditing the network installation— network planning checklist 1. Is there a network installation plan? 2. Is the plan sufficiently detailed? 3. Does the network manual contain detailed provisions for disaster preparedness? 4. Are network testing procedures, clearly documented? 5. Is confidentiality of network traffic, adequately addressed? 6. Is documentation available for all networking equipment? 7. Is the documentation maintained on a regular basis? XVI. Checklist for network services and application coordination 1. Are all network services catalogued? 2. Are users restricted to using only authorized services? 3. Are users protected from each other? (a) Are only authorized users allowed to update data? (b) Are “super” users strictly monitored? 4. Are users restricted to performing only authorized functions? (a) By time of day? (b) Day of the week? (c) Terminal? (d) User ID? (e) Transaction? 5. Are user identification techniques in place? 6. Is unusual activity reported and investigated?		

SUMMARY

In this chapter, we started our discussion with an introduction to the 'network', its classification, both on the basis of its spread and application architecture. After this brief introduction, we discussed in detail, the various types of network topologies, their pros and cons, and the selection criteria for different topologies. The control-specific issues, relating to network cabling, i.e. the type of cables or carriers, their advantages and disadvantages, the selection criteria for different carriers, were also discussed.

We then discussed various network devices like the hub, switch, bridge, and router and control-specific issues, related to these. After a brief idea of the network, we introduced the readers to one of the very fundamental and interesting aspects, i.e. the IP addressing. The various types of IP addressing schemes and the implications of all these have also been discussed in detail. After this, it is expected that the readers will have a fundamental idea about a network, in particular, an IP network. So, we discussed the various risks associated with network operation and the related controls. While discussing the controls, we did not limit our discussion to the technical controls. The various management controls, related to network operation were also discussed. During our discussions on technical controls, we emphasized the firewall and the Intrusion Detection System. With all that has been discussed so far, the reader will have a thorough idea about network operations, the associated risks, and the need for various controls. We also introduced the readers to the subject of auditing the network, with detailed steps, that the auditor should follow, while doing this exercise. At the end, we gave a very comprehensive checklist for network audit.

REVIEW QUESTIONS

1. Describe different type of networks both, on the basis of its geographical spread and application architecture.
2. What are the different types of network topologies? Describe each one of them with the help of diagrams and give a comparative analysis of all the topologies.
3. What is an Open System Interconnect (OSI) model in the network technologies? Describe each layer and its function in this model.
4. What are different types of network cabling? Describe the advantages and disadvantages of each type.
5. What are the different types of network devices? Describe four such devices and give their comparative analysis.

6. What is an IP address? How does this type of addressing ensure network communication?
7. Describe different kinds of threats to a network.
8. What are the different kind of controls to counter various threats to the network?
9. Describe the different kinds of firewalls and give their comparative analysis.
10. What are the different steps required to audit a network? Write briefly about each step.

MULTIPLE CHOICE QUESTIONS

1. Social engineering is related to:
 - (a) Engineering
 - (b) Sociology
 - (c) Computer science
 - (d) Hacking computer systems
2. Which one of the following is one of the differences between LAN and WAN?
 - (a) WAN uses layer 3 devices, whereas LAN does not
 - (b) WAN connects to the Internet, while LAN does not
 - (c) WAN is more secure than LAN
 - (d) In case of LAN, all the components are owned by the organization, which is not the case in WAN
3. One of the disadvantages of peer-to-peer network is:
 - (a) Difficulty in troubleshooting
 - (b) Easy to hack
 - (c) Poor availability
 - (d) Poor management
4. Which is the best way of defining a network topology?
 - (a) Physical layout of the devices of the network
 - (b) Physical and logical layout of the devices of the network
 - (c) Logical layout of the devices of the network
 - (d) A network layout diagram
5. When conducting an audit of client-server database security, the IS auditor should be MOST concerned about the availability of:
 - (a) System utilities

- (b) Application program generators
 - (c) Systems security documentation
 - (d) Access to stored procedures
6. Which of the following network topologies yields the GREATEST redundancy, in the event of the failure of one node?
- (a) Mesh
 - (b) Star
 - (c) Ring
 - (d) Bus
7. Which of the following is NOT an element of a LAN environment?
- (a) Packet switching technology
 - (b) Ring or bus topology
 - (c) Private circuit switching technology
 - (d) Ethernet technologies
8. An organization is about to set up a computer network in a new office building. The company has 300 users, located in the same physical location. There is no need for any external connection/interface. Which of the following network configurations would be the most effective for problem resolution?
- (a) Bus
 - (b) Ring
 - (c) Star
 - (d) Mesh
9. Connection-oriented protocols in the TCP/IP suite are implemented in the:
- (a) Transport layer
 - (b) Application layer
 - (c) Network layer
 - (d) Physical layer
10. Congestion control in the network is best handled by which OSI layer?
- (a) Network layer
 - (b) Data link layer
 - (c) Application layer
 - (d) Transport layer
11. What is the main disadvantage of a star network?
- (a) Difficult installation

304 *Information System Audit and Assurance*

- (b) Low scalability
 - (c) Expensive
 - (d) Single point of failure
12. A hub has:
- (a) One collision and multiple broadcast domain
 - (b) One broadcast and multiple collision domains
 - (c) Multiple collision and multiple broadcast domains
 - (d) Single collision and single broadcast domain
13. IP address is essential for:
- (a) Communicating between two computers in one LAN
 - (b) Communicating between two computers in different LAN
 - (c) Communication inside a computer
 - (d) Communication between two computers
14. Which of the following statements is true for a private IP address?
- (a) A confidential address, allotted exclusively to one organization
 - (b) The addresses allotted to a particular organization
 - (c) The addresses allotted to a closed-user group
 - (d) An address that cannot be used by the Internet
15. A subnet mask is used:
- (a) For communicating between two subnets
 - (b) For determining the default gateway
 - (c) For determining whether the packet is for the same network or not
 - (d) For hiding the network
16. A hub is a device that connects:
- (a) Two LANs using different protocols
 - (b) A LAN with a WAN
 - (c) A LAN with a MAN
 - (d) Two segments of a single LAN
17. Which of the following line media would be MOST secure, in a telecommunication network?
- (a) A broadband network digital transmission
 - (b) Baseband network
 - (c) Dialup
 - (d) Dedicated lines

18. Which of the following firewalls, provides the greatest degree and granularity of control?
- (a) Application gateway
 - (b) Packet filter
 - (c) Screening router
 - (d) Circuit gateway

DISCUSSIONS AND RESEARCH QUESTIONS

1. Peer-to-peer networks are called networks for the network administrators. Discuss.
2. What is “classless” IP addressing? What does this scheme of addressing mean?
3. What is the basic difference between brute force and dictionary attack, on the password?
4. Describe the differences between a Denial of Service (DOS) and Distributed Denial of Service (DDOS) attack.
5. Management controls are the limiting factor for all other technical controls to counter the threats to the network. Discuss.
6. It is more important to know about firewalling as a function than knowing about firewall as a product. Discuss.

EXERCISES

1. Write a checklist for auditing a router.
2. Describe how a Class C address (192.168.10.0, subnet mask 255.255.255.0) can be sub-netted to create 5 subnets, with the following number of hosts in each subnet. Write the range of each subnet.
 - (a) Subnet #1 30 hosts
 - (b) Subnet #2 22 hosts
 - (c) Subnet #3 27 hosts
 - (d) Subnet #4 25 hosts
 - (e) Subnet #5 20 hosts
 - (f) Can subnet #5 be increased to 35 hosts? If so, how?
3. Your organization has an IP address range (172.16.1.0 subnet mask 255.255.255.0). Suppose there are 9 departments in your organization and each department has 12 systems that need to be networked. How

will you go about the task? What is the maximum number of systems in each department (assuming equal number of systems in each department)?

4. Write a checklist for auditing a firewall, which exists at the Internet gateway of a banking organization.
5. A service providing organization namely, Net Services Limited (NSL), provides services relating to networking, applications and consultancy, to various organizations, including its sponsors (principal). One of the services provided by NSL is Internet connectivity. Organizations that opt for such services, would have to connect their network to the NSL's network, which has a secure gateway to the Internet. Similarly, the network of the sponsor is also connected to NSL's network for Internet connectivity and other applications.

The demand for the Internet connectivity grew so much, that there was a considerable reduction in the response time, which resulted in the sponsors becoming very unhappy with NSL. Consequently, the sponsors asked NSL to consider either increasing the bandwidth or give a dedicated channel to them. The CEO of NSL asked the networking Group to propose various options for solving this problem. The options put forth by the networking group are as below:

- (a) Increasing the bandwidth
- (b) Giving a dedicated channel to the sponsor
- (c) Asking the sponsor to take a dedicated Internet connectivity/channel from a reputed ISP at his/her, end so that the Internet traffic of the sponsor will not come to the NSL

Required: You being the head of internal IS Audit, are called by the CEO to apprise him of the security implications of all the above proposals. Prepare a report to this effect.

7

Internet Banking—Risks and Controls

-
- ❖ Internet banking—A multiple-delivery channel
 - ❖ Introduction to web technology
 - ❖ Issues related to web technology
 - ❖ Types of Internet banking
 - ❖ Secured Internet banking architecture
 - ❖ Internet banking in a centralized environment
 - ❖ Internet banking in a distributed environment
 - ❖ Multilayered security model
 - ❖ Risks and control in various components
 - ❖ Auditing Internet banking
 - ❖ Basics of penetration testing
 - ❖ Checklists for auditing Internet banking
-

INTERNET BANKING—A MULTIPLE-DELIVERY CHANNEL

The dotcom hype in 1996 held out the promise that the Internet could be used for any kind of commerce activity and banking would be no exception. All over the world, there was a rush among existing banking organizations to deliver their products and services through the Internet— an inherently insecure channel. Not only banks, but non-banking institutions and IT companies, also jumped into the fray for delivering their financial products through the Internet.

There came a time when the purpose of the existence of a brick and mortar bank started to be questioned. The Internet started being seen as a threat to banking organizations as it had the ability to intermediate between the debtor and the creditor, which is the basic function of a bank. All this hype however,

did not last long. The first few, pure play Internet banks did not show much promise. And the first wave of Internet banking soon lost its vigor. But the potential of the Internet as a delivery channel did not dissipate. The study conducted by the consultants Booz-Allen and Hamilton, on the reduced transaction cost, is noteworthy in this context. The study shows that the cost of a customer walking into a branch and using a teller is USD 1.01, while the cost of conducting the same transaction on the Internet is a tenth of that, i.e. USD 0.10. A similar study conducted in India (* Source: India Research May 29, 2000, Kotak Securities), reveals that the cost of banking service, provided through the Internet, forms a fraction of the costs incurred through conventional methods. Rough estimates assume teller cost at Re. 1 per transaction, ATM transaction cost at 45 paise, phone banking at 35 paise, debit cards at 20 paise, and Internet banking at 10 paise, per transaction.

The Internet technology, in the meantime, grew leaps and bounds. The same technology, which was considered to be inherently insecure, now provided the means for making this a secured channel. And various activities, including electronic bill payment, E-cheque payment, stock trading, FOREX transactions, etc. were carried out through this channel. Banks all over the world started using this as a multiple-delivery channel. Regulators across the globe also realized the opportunities and strengths, of this channel and issued various guidelines for making it more vibrant and secure. Thus, the second wave of Internet banking, as a multiple-delivery channel, became pervasive and has come to stay, especially in the banking arena, across the globe.

INTRODUCTION TO WEB TECHNOLOGY

Before discussing the various issues related to Internet banking, let us first know the basics of web technology, which is used by all internet-enabled applications, including Internet banking.

How a Static Web Page Works

In the case of the web technology, the client is a browser (say Internet explorer, Netscape, opera, etc.) which after taking the URL (Universal Resource Locator), for example, <http://xyzbank.com>, as input, tries to reach the web server. The web server is a piece of utility software or system software, for example, IIS (Internet Information Server), Apache, etc., which sits on the operating system, called the web host, in web technology parlance. Now, the client's request reaches the web server through any communication media and searches for the home page. Once the home page, which is written in Hyper Text Markup

Language (HTML) is found, it is sent to the client (browser), through the same communication channel, either through the intranet or through Internet. The client (browser) is designed to show the HTML content, the way usually we see it. As the HTML code, present in the web server, is physically sent to the browser, we can view the source in the browser with the help of the “view source” option. Whatever has been discussed above, is about how a static web page works.

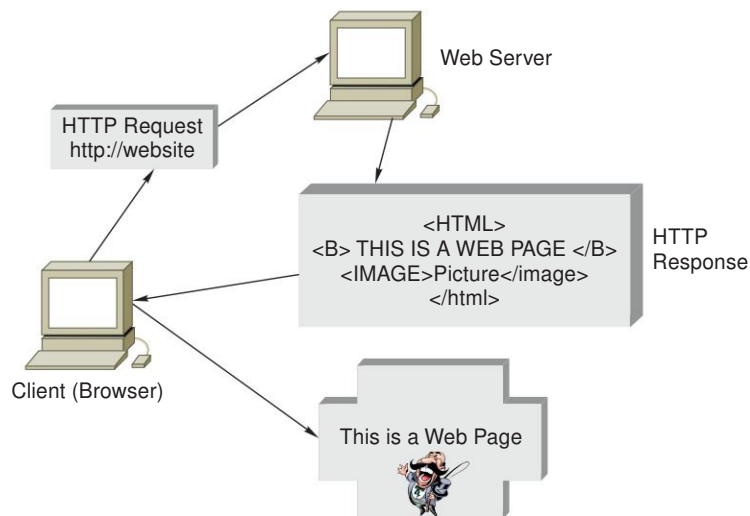


Fig. 7.1 Static web page

How the Dynamic Web Page Works

In case of dynamic content, the home page, which initially comes to the browser, takes some input from the user, for example, the hall ticket number and the name of the examination and takes this string to a backend database. It then gets the query redressed, say the result pertaining to that particular hall ticket number, and displays this to the user, through the browser. This is also similar to the balance enquiry application of Internet banking. The string from the browser to the backend database can go through many tiers like, application server, middle ware, etc., depending on the application architecture. Now let us see how this dynamic page works.

The browser as usual gets the home page and the user enters some values. These values go to the web server and are interpreted by any language designed for interpretation, like, ASP, Perl, etc. From here, it travels through different language layers, depending on the application architecture, fetches the query,

converts it again to HTML format and sends it to the browser. So, ultimately, what goes to the browser, is in HTML text, which is the output of some intermediate operations.

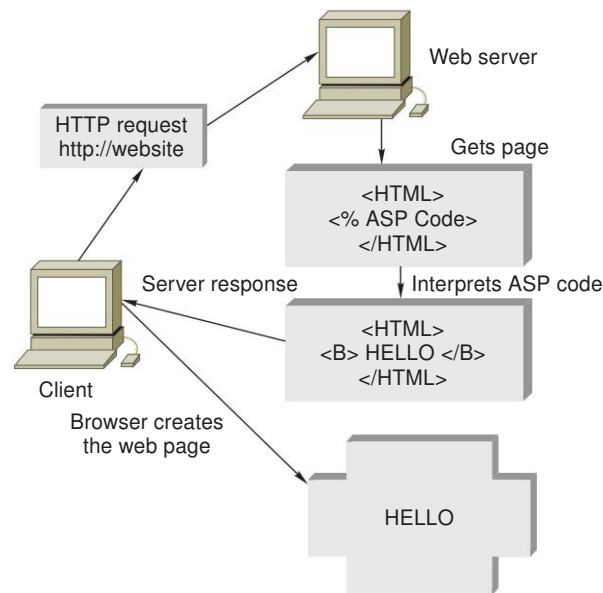


Fig. 7.2 Dynamic web page

The Internet

After having read the bare minimum basics about the web technology, we have come across some new concepts (that may be too simple for the *techies*), viz. HTTP, HTML, web server, web host, etc. Now, let us use these concepts further and describe the infrastructure components, required for connecting to the Internet.

The basic prerequisite for offering Internet banking is to get connected to the Internet. Now, let us understand how we can get connected to the Internet. What we today call the Internet, began as a government-funded network called the ARPANET (named after ARPA, the Department of Defense's Advance Research Project Agency, USA), which is now known as DARPA. The "backbone", i.e. the core that connected all the edge networks was funded by the Government. These edge networks were owned and maintained by universities, research organizations, and government agencies and all these were interconnected with the help of ARPANET. This inter-networking of many IP networks through a core backbone, gave rise to a popular and very

familiar term, i.e. *Internet*. So, the modern Internet has been built from a collection of privately built and operated, backbone networks that are interconnected at major demarcation points, around the world. The companies that own and provide access to these networks are called Internet Service Providers (ISP). These ISPs can be as big as AT&T that operates global high speed backbone and are called backbone ISP. The smaller, region-based ISPs serve individual countries or states, like, the VSNL (Videsh Sanchar Nigam Limited) and other similar companies in the case of India. Down the line, there are smaller service providers, who are connected to the regional providers.

HIERARCHY OF ISPs

Banks should approach an appropriate ISP for providing a link to the Internet. This link is basically, physical access to the Internet. Nowadays, this physical access comes in many forms (Table 7.1).

Now, after knowing the different ways by which, the ISPs provide connection to the Internet, let us discuss the other things that an ISP should provide, from an Internet banking perspective and also, the security implications of choosing a particular ISP.

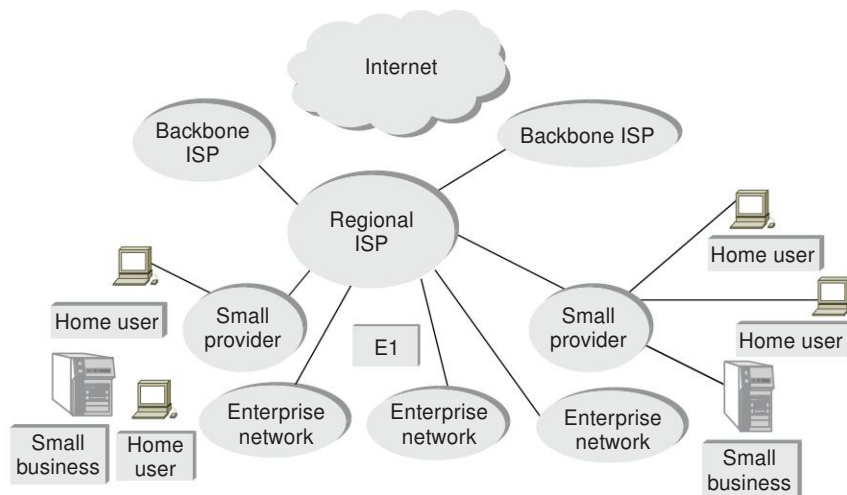


Fig. 7.3 Hierarchy of ISP

Table 7.1

Carrier	Connection speed	Requirement
Dial-up modem	Maximum 56 Kilo Bits Per Second (KBPS)	Home user.
ISDN (Integrated Services Digital Network)	Two 64 KBPS channels that can be used for voice, fax or data. Some ISPs, support ISDN and strap their 64 KBPS channels, to give 128 KBPS connection to the Internet.	Home users, small organizations, Backup for large organizations.
DSL (Digital Subscriber Loop)	Broadband connection. This advanced technology, allows the phone line to be used both, as a normal telephone line and for full time Internet access. High speed (1 to 2 MBPS) data flows from the Internet to the end-users, while a low very little data speed (56 KBPS) for the outbound traffic (Asymmetric)	This asymmetric service works on the assumption that usually, the consumer spends a lot of time in downloading information and actually very little data.
Cable modem	High speed (1 to 2 MBPS), asymmetric.	Home user.
T1/ T3 (E1 and E3 in India)	Within the telephone network. High bandwidth in MBPS E1 from 2 mbps E3 45 MBPS.	Enterprise customers.
OC3 and higher	High-speed, fiber-optic links, starting from 155 MBPS.	Serious users, within ISP backbone.
Ethernet	Usually 100 MBPS, provided by ISPs that provide collocation of servers.	Enterprise customers.

Apart from a link to the Internet, the bank needs one or a whole set of public IP addresses (about which you have already learnt in the chapter “Network security and control”), for the web servers and if required, the mail server will need an interface to the Internet. We also need the IP address of one or more Domain Name Servers (DNS), which will act as a telephone book for the Internet. The DNS, helps in translating the URL, for example, <http://www.xyzbank.com> to the public IP address say 1.2.3.4, which is the address of the web server of ‘XYZ’ bank. Depending on the requirement and

contract terms, the ISPs provide some E-Mail accounts, disk space for web page, and also security features like, firewall and intrusion-detection systems (IDS), etc.

The security features provided by the ISP, are normally for protecting the ISP from you and not to protect you from everyone else on the Internet. The ISP would expect you to operate within the bounds of their Acceptable Use Policy (AUP). In fact, such kind of monitoring by ISPs, is good for all, as the ISP can provide an insight into, whether any of its clients' systems are being used, to hack the systems of others. The ISPs however, would not be of any immediate help, if your system has been hacked. It may happen, that the ISP may isolate you from others, to preventing the occurrence of attacks on other systems. The purpose of stating the above, is to just drive home the fact, that depending on an ISP for security, is not sufficient. You need to get your own house in order.

The availability of the Internet link is very important from an Internet banking perspective. So, while obtaining the links, it should be ensured that there is sufficient redundancy. From a control perspective, it is always advisable to obtain the links from two different providers (ISP) and implement load sharing and redundancy, between these links, either by a separate load balancer or by implementing the Border Gateway Protocol (BGP), at the respective ISP's site.

ISSUES RELATED TO WEB TECHNOLOGY

The World Wide Web

The World Wide Web (WWW), is 'a network of web servers, which provides a mechanism, to link pages with content, to other related pages, over the existing Internet'. Currently, most of the web servers, provide read access, to a file system of HTML files (static content) or a database, serving active content. Active content uses interpreted and binary codes that execute on the browser. Consequently, the commercial web servers have become very large and complex, code bases.

JAVA AND JAVA BEANS

Java is a programming language, developed at Sun Microsystems, to program consumer products. First launched in 1995, it was in 1996 that Java really gained strength. Java, is loosely based on C++. It was stripped down to a bare minimum, in order to be compatible with the limited space that the chips in

hand-held devices offered, and was designed to allow programmers to support dynamic, changeable hardware, more easily.

Java is, 80 per cent compiled and 20 per cent interpreted language. Its portability is achieved by generating a byte code that is executed at run time. Java applets are byte codes that are downloaded and executed, within a browser. Most browsers and servers support Java runtime interpreters and just-in-time compilers.

Java Beans is Sun's component architecture and the API set for building reusable Java components. The Java Beans component model, provides component interface publishing and discovery, event handling, persistence, layout, and application-builder support. Using Java Beans, developers define, independent components that can be reused in a variety of ways, to create a new browser and even non-browser applications.

ACTIVE X AND ACTIVE DESKTOP

ActiveX is Microsoft's component strategy for building Windows applications and browser-based applets. ActiveX is based on Microsoft's 'Object Linking and Embedding (OLE)' object standard and Component Object Model (COM). ActiveX enables software components to interact with one another in a networked environment, regardless of the language in which they were created. ActiveX uses binary object code, instead of Java's byte code that is downloaded into browsers. Java Beans and ActiveX are competing for the same computing space.

An active desktop, utilizes ActiveX on the desktop (browser) and server (active server). Microsoft's Internet Explorer browser, incorporates this technology. This allows the browser to pull and push data, depending on the applications. The active server, stores a user's personalized information. When certain business events transpire (e.g. new mail messages, document updates), the browser is notified and it selects the appropriate function.

CLIENT SERVER VS. WEB

Traditional client server development environments, can rely on persistent connections, between clients and servers. Web communications, using HTTP, are intermittent, meaning that they are constantly being established, torn down and re-established, as the browser requests pages and objects, over the network. This makes keeping state, between requests, next to impossible. Alternative methods, like, cookies, and modified URL links, are all that the technology offers, at the present time. This lack of connection state, is a major security limitation with HTTP.

Currently, the HTTP protocol only supports basic authentication (clear text username with an unencoded password). HTTP roots are from the Internet; hence, it offers no more security than the current suite of Internet applications (e.g. FTP, TELNET, and SMTP). Each time a web page is accessed (which requires authentication), the web server performs an authorization check. If an empty authorization header field is sent (status code 401-Unauthorized), the user is prompted for a username-password pair. The browser caches the authorization information locally, for each given URL realm. This allows users to authenticate once, for a given resource.

Most modern client server applications (SAP, Novell and NT Server, Windows 2000), use encrypted passwords and strict access control binding.

DELEGATION OF AUTHORITY

The delegation of authority is *'the process of transferring authority to a given principal, in order to perform a certain action that requires access control'*. Authorization, specifies the resources that are to be accessible to a principal, e.g. user, process, role, and job title. A resource could be a transaction, account, menu, or something that one wants to protect. The user and/or process that requests access to a resource, is known as a principal. An Access Control List (ACL) is associated with each resource, listing the individuals (principals), authorized to access the resource, along with the access rights that have been authorized, e.g. query, debit, and trade. An ACL manager, processes the request from the principal, and compares it with the resource's ACL.

Currently, in the WWW technology, no one is addressing authorization, in a standard manner. Most authorization is performed at the operating system level, e.g. file and directory, and at the DBMS level, e.g. tables. This requires web application developers, to develop specific security codes, to provide a fine granular access to corporate resources. The benefit of this standard is that it provides application developers with a common authorization API, that allows them to get the same security level, without writing specific codes. This allows the application, quicker time to market, and also, ease of maintenance.

Most authorization decisions are based on a relationship with a given principal name. This name, could be part of a role, e.g. group for a given job title, within an organization. In most cases, access to resources is not performed from a principal name, but from a job title or role name. Associative access control mechanisms consists of resource Access Control Lists (ACLs) or user capability lists, i.e. resources to which a user has access. This access decision is based on the permission(s), e.g. credit, debit, etc., derived from the intersection of the resource and role pair. An ACL consists of roles and permissions for a

given object. Conversely, a capability list consists of resources that a role has access to.

Logical access control is based on the accumulation of a given action, over a period of time, e.g. thresholds, sequences, or some logical combination of these. It is assumed that an associative check will be performed, before the logical check. This will allow organizations, to limit the principal's access, based on credit or trade limits, or necessary sequences, to complete a transaction, e.g. bank authorization before purchase.

ACTIVE CONTENT PROBLEMS

Remote distribution and execution of software on the Intranet is less risky, than on the Internet. Java, Java Beans and ActiveX are paving the way for this technology. ActiveX is a binary object code, based on Object Linking and Embedding (OLE) that runs inside the browser. It is not constrained by the browser. Once it is enabled, it can perform any operation that an OLE-based application can perform. The differences between, executing client applications and ActiveX, are negligible. ActiveX runs a lot faster than Java, but nothing prevents it from wrecking havoc on your desktop. An example of this, is an ActiveX control called 'Exploder', which has shut down Windows 95.

AUTHORIZATION

To design authorization properly, in an enterprise, one has to employ some basic security concepts like, "separation of duties", "least privilege", and "individual accountability". *Separation of duties* is the practice of dividing the steps in a critical function, e.g. approving monetary transactions, audit reviews, among different individuals. The *least privilege* principle is the practice of restricting a user's access to data files, processing capability, or peripherals, or in the case of type of access (read, write, execute, delete), to the minimum, necessary to perform the job. *Individual accountability* means holding someone responsible for his/her actions.

Accountability is normally accomplished by, identifying and authenticating users of the system and subsequently, tracing actions on the system to the user, who initiated them. The problem is, integrating security mechanism with the existing Intranet design.

ACTIVE CONTENT SOLUTIONS

The browser must control all active content processing. This includes regulating the download, enabling of ActiveX controls or external plug-ins, and executing

ActiveX scripts and Java. Browsers must also control, from who and where they accept software, i.e. are they trusted sites and software publishers? This is accomplished by the browser by storing the public keys of the sites and by digitally signing the active content, before it downloads. If the code is not signed, the browser by default, should not download it.

Browsers protect themselves from Java, using a strict applet sandbox-style, security measure that resides in the Java virtual machine. The enforcement happens, after the byte code has been downloaded, verified, and instantiated by the class loader. The applet security manager takes over the task of monitoring all operations, from this point. It is established at startup, and thereafter, it cannot be replaced, overloaded, overridden, or extended. Applets cannot create or reference their own security manager. Applets are also prevented from reading and writing files on the client file system, and from making network connections, except to the originating host.

Microsoft's Authenticode, addresses this risk, by identifying who published the software, before it is downloaded, and verifying that no one tampered with it, before or during the download process. This however, does not solve the problem of introduction of malicious codes into the browsers, e.g. virus or Trojan horse. You should therefore, be on the look out for an online virus scanner, for ActiveX controls. Other than the aforementioned techniques, the only way to control ActiveX is through procedural means, e.g. security awareness training.

It is likely that the use of web technology jargon, might have made you a little uncomfortable. So, let us now, go back to something more familiar, viz. banking. Let us also discuss the types of Internet banking and how to correlate it with web technology, about which we have learnt above, in appropriate places.

TYPES OF INTERNET BANKING

As has been discussed earlier, Internet banking is the use of the Internet, as a remote delivery channel for banking services, including traditional services, such as opening a deposit account or transferring funds among different accounts, as well as new banking services, such as, electronic bill presentation and payment, which allow customers to receive and pay bills through a bank's website.

An existing bank, with physical offices, can establish a website and offer its customers Internet banking, in addition to its traditional delivery channels. The range of products and services offered by different banks vary widely, both, in their content and presentation.

Broadly, the levels of banking services offered through the Internet can be categorized into three types:

- The basic service is the *banks' website*, which disseminates information on different products and services, offered to customers and members of the public in general. It may receive and reply to the customers' queries through E-Mail (as in case of the static website, discussed above). Such kind of Internet banking is static and does not use any backend database
- In the next level, are '*simple transactional*' websites, which allow customers to submit their instructions, applications for different services, queries on their account balances, etc., but do not permit any fund-based transactions on their accounts (as in case of the Dynamic website discussed earlier). Such simple transactional websites could be using a database, but are unlikely to be using the core database of the bank
- The third level of Internet banking services, are offered by '*fully transactional*' websites, which allow the customers to operate their accounts for transfer of funds, payment of bills, subscribing to other products of the bank, to transact purchase and sale of securities, etc. (as in case of the dynamic website discussed earlier). Such kinds of Internet banking websites, usually use the core database of the bank
- The fourth type of Internet banking services, which never quite picked up are "pure play" Internet banking portals, having no brick and mortar branch. Examples of this kind of 'Internet-only' banks are the egg, Smile, in UK and Wingspan Bank, in USA

All the above forms of Internet banking services, except the fourth, are offered by traditional banks, as an additional method of serving the customers or by new banks, that deliver banking services, primarily through the Internet or other electronic delivery channels, as value added services.

FEATURES OF INTERNET BANKING

Some of the unique features of Internet banking are:

- The non-existence of the traditional geographical barriers, as it could reach out to customers of different countries, each having its own legal jurisdiction. This has raised the question of jurisdiction of law/supervisory system, to which such transactions should be subjected
- The emergence of new risks and the challenge to control them, while at the same time, increase in some of the other traditional risks

- Security of banking transactions, validity of electronic contract, customers' privacy, etc. which have all along been concerns of both bankers and supervisors, have assumed different dimensions, given that the Internet is a public domain, not subject to control by any single authority or group of users

The concerns in Internet banking, arise mainly, out of the unique features, outlined above. These concerns can be addressed under three broad categories, viz. :

- Legal and regulatory issues
- Security and technology issues
- Supervisory and operational issues

Of these three, the first two can more or less be taken care of by adhering to legal and regulatory guidelines, but the issues related to security are very critical. When we say security; it means the security of the customers' accounts, security of the bank's funds, the security of each and every transaction that takes place, security of the bank's system, and the reputation of the bank.

Although 'security' in Internet banking is a multi-layered concept, i.e. dependant on many components, yet the designing of the basic architecture is of prime importance. This architectural design, helps in applying security to the various security layers of Internet banking, in an optimal way. Therefore, in the following section, we will discuss the various architectural options available in Internet banking and then deliberate on the multi-layered security model.

The designing of the architecture is very much dependant on the Internet banking functional model, i.e. either centralized (core) banking solution or distributed banking solution. First of all, we will describe a generic architecture and then discuss, the various architectural options available, both, in the centralized and distributed environments.

GENERIC ARCHITECTURE

The generic architecture, is based on the following presumptions:

- Internet banking is a delivery channel for a centralized banking solution
- The Internet banking web server is hosted by the bank, in its own data center
- The application architecture is four-tier, i.e. control from the web server reaches the database server, through the application server and middleware
- The bank's data center is physically located in the same building, whether or not there are other functional areas also in existence

Depending on the presumptions mentioned above, the generic architecture has been depicted in Fig. 7.4

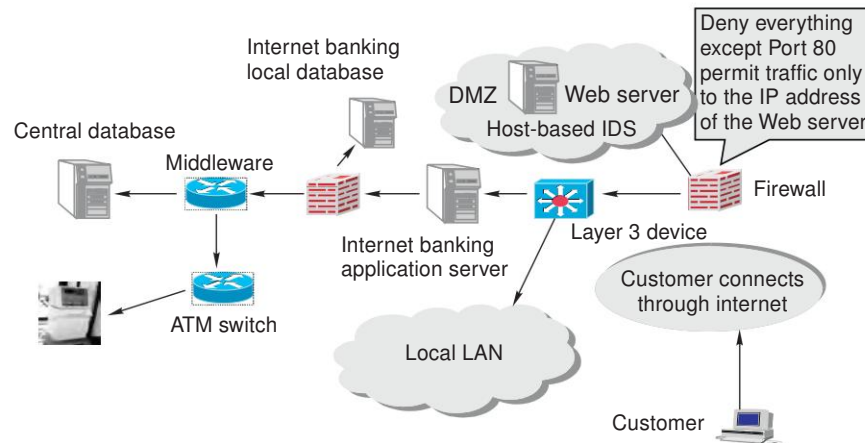


Fig. 7.4 Generic architecture of Internet banking

Note: In the diagrams that follow, *LAN* is Local Area Network, *VLAN* is Virtual LAN, *WAN* Wide Area Network, *DMZ* is De-Militarized Zone, *WS* is Web Server, *MW* is MiddleWare, *DB* is Database, *App Srv* is Application Server, *IDS* is Intrusion Detection System(s), *ATM* is Automated Teller Machine, *CUG* is Closed User Group, *INFINET* is INdian FINancial NETWORK, *TSP* is Third-party Service Provider and *IB* is Internet banking.

With this generic architecture serving as a reference, we now examine the different options that banks have at their disposal, based on their banking solution preference, i.e. centralized or distributed.

INTERNET BANKING IN A DISTRIBUTED ENVIRONMENT

In this environment, the database is distributed across the various branches of the bank. The bank has, at its disposal, three options by which it can setup Internet banking.

Option 1: Bank has its Website Hosted at its Own Location (Data Centre)

The following assumptions are made in this case:

- The database is localized
- Multi-platform application

- Middleware at each branch
- The bank has its own WAN
- Own web hosting.

This scenario can be represented diagrammatically as shown in Fig. 7.5.

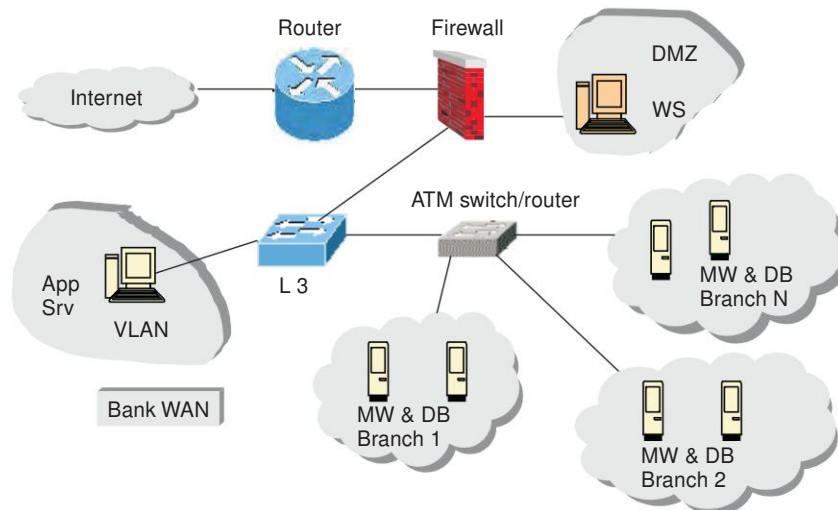


Fig. 7.5 Distributed environment: Internet banking architecture

In such a scenario, the advantages and disadvantages to the bank are, as given below:

- *Advantages:*
 - No single point failure
 - Own location of data centre means, no involvement of third-party
- *Disadvantages:*
 - Latency, induced due to the amount of routing involved, because of distributed architecture
 - Failure of a single branch means, the inability of the customers of that branch to make use of Internet banking

Option 2: Bank has its Website Hosted in a Closed User Group (CUG) Environment

In this scenario, the bank will host its website in a location that is part of a CUG network, like, Indian Financial Network (INFINET). The application

server is hosted at the bank's location which has connectivity with the CUG network. Now, there are two sub-options available:

- The bank has its own WAN
- The bank uses the CUG network

Option 2a: The Bank has its Own WAN

The following assumptions are made in this case:

- The database is localized
- Multi-platform application
- Middleware at each branch.
- The bank has its own WAN

In this scenario, the request will travel over the CUG network, to the application server of the bank and from the application server, the request will travel over the WAN of the bank, to the database server of the intended branch. This is depicted as follows:

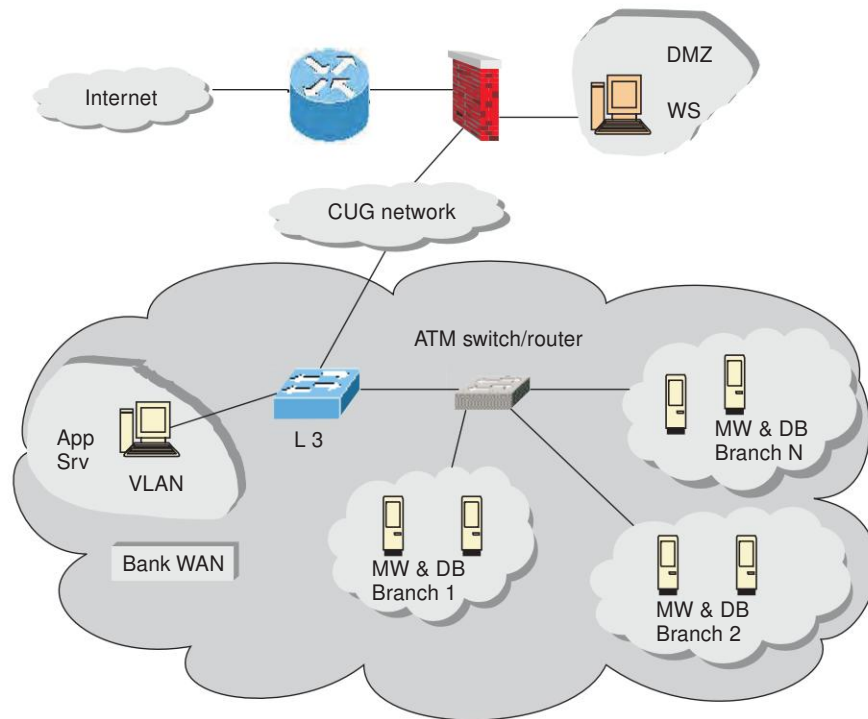


Fig. 7.6 Distributed environment Internet banking architecture

Option 2b: The Bank Does Not have its Own WAN and Uses the CUG Network

The following assumptions are made in this case:

- The database is localized
- Multi-platform application
- Middleware at each branch

In such a scenario, the advantages and disadvantages to the bank are, as given below:

- *Advantages:*
 - No major investment in network infrastructure
 - No dependency on any third-party for data centre
- *Disadvantages:*
 - Latency, induced due to the amount of routing involved, because of distributed architecture
 - Failure of the CUG network paralyses Internet banking
 - Failure of a single branch means, the inability of the customers of that branch to make use of Internet banking

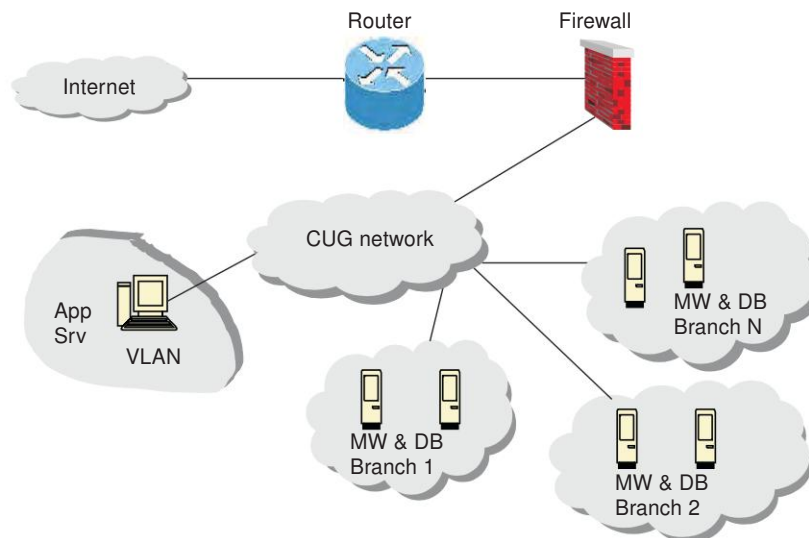


Fig. 7.7 Distributed environment: Internet banking architecture

Option 3: Web Hosting by TSP With No CUG Network

The following assumptions are made in this case:

- Website is hosted by a third-party service provider
- The database is localized
- Multi-platform application
- Middleware at each branch
- Bank has its own WAN

In such a scenario, the issues, advantages and disadvantages to the bank are, as given below:

- *Advantages:*
 - Pay and use facility of the data centre
 - No cost incurred on infrastructure establishment
- *Disadvantages:*
 - Dependency on third-party for the data centre
 - Failure at data centre means, failure of Internet banking
 - Failure of the distributed architecture

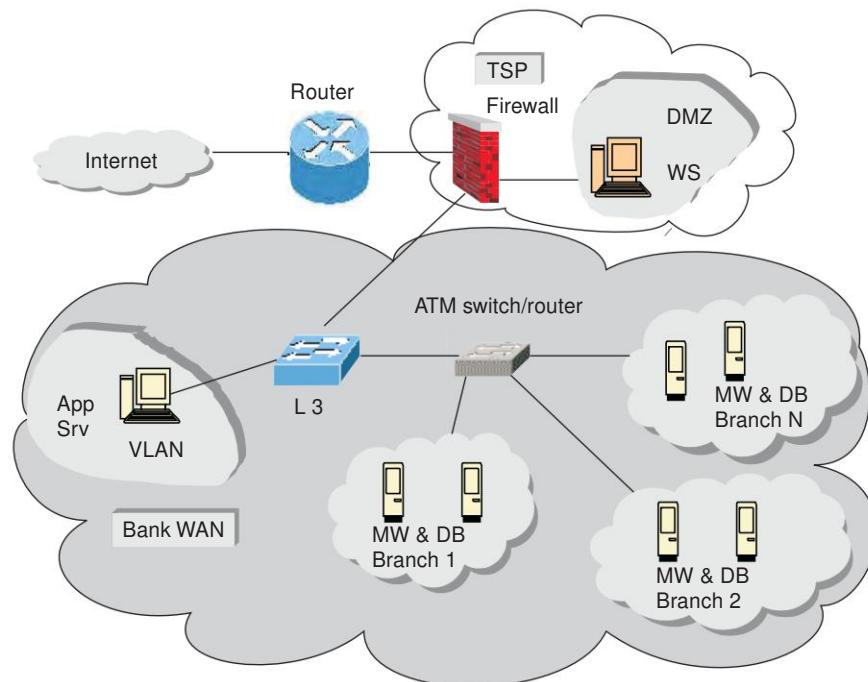


Fig. 7.8 Distributed environment: Internet banking architecture

INTERNET BANKING IN A CENTRALIZED ENVIRONMENT

In this environment, the bank has a centralized database. The bank has, at its disposal, three options by which it can set up Internet banking.

Option 1: Bank has its Website Hosted at its Own Location (Data Centre)

The following assumptions are made in this case:

- The database is centralized
- Single-platform application
- Single middleware at the data centre
- The bank has its own WAN
- Own web hosting, at own data centre

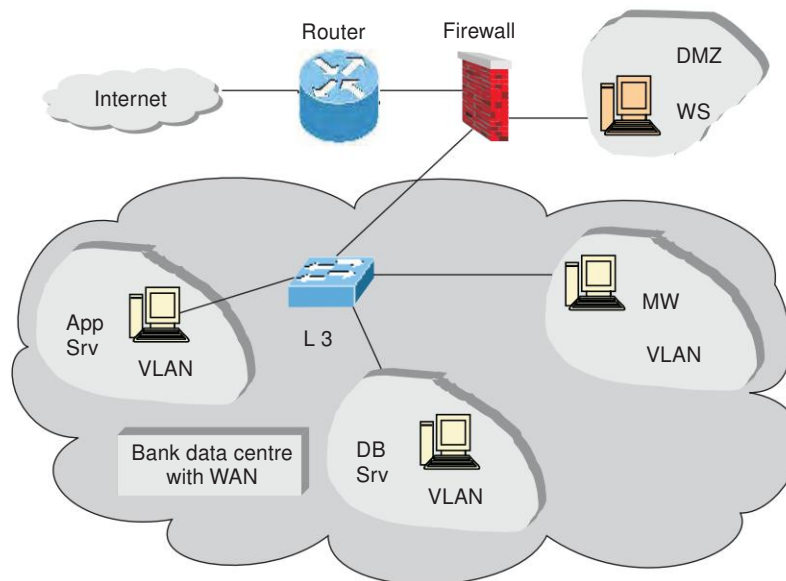


Fig. 7.9 Centralized environment: Internet banking architecture

Option 2: Bank has its Website, Hosted in the Data Centre of the CUG Network

In this scenario, there are two sub-options:

- The website alone, is hosted in the data centre of the CUG network

- The whole setup of Internet banking (application server and database server), is hosted in the data centre of the CUG network

Option 2a: Only the Website is Hosted at CUG Data Centre

The following assumptions are made in this case:

- The database is centralized
- Single-platform application
- Single middleware at the data centre
- Web hosting at data centre of the CUG network

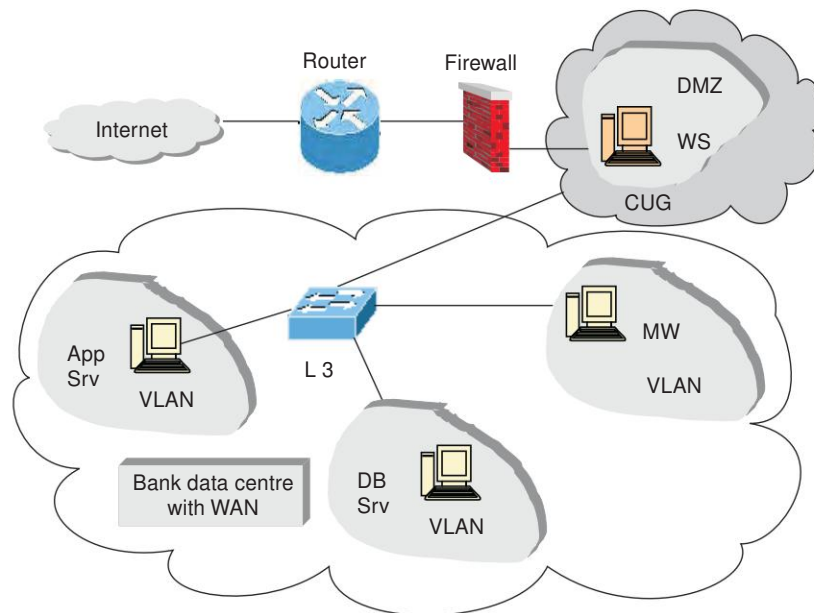


Fig. 7.10 Centralized environment: Internet banking architecture

In such a scenario the advantages and disadvantages to the bank are, as given below:

- *Advantages:*
 - No need for setting up data centre
- *Disadvantages:*
 - Maintenance of the website by the third-party

Option 2b: Whole IB Setup is in the Data Centre of CUG

The following assumptions are made in this case:

- The database is centralized
- Single-platform application.
- Single middleware at the data centre
- The bank may have its own WAN, but the Internet banking setup is hosted in the data centre of the CUG
- Web hosting at data centre of the CUG network

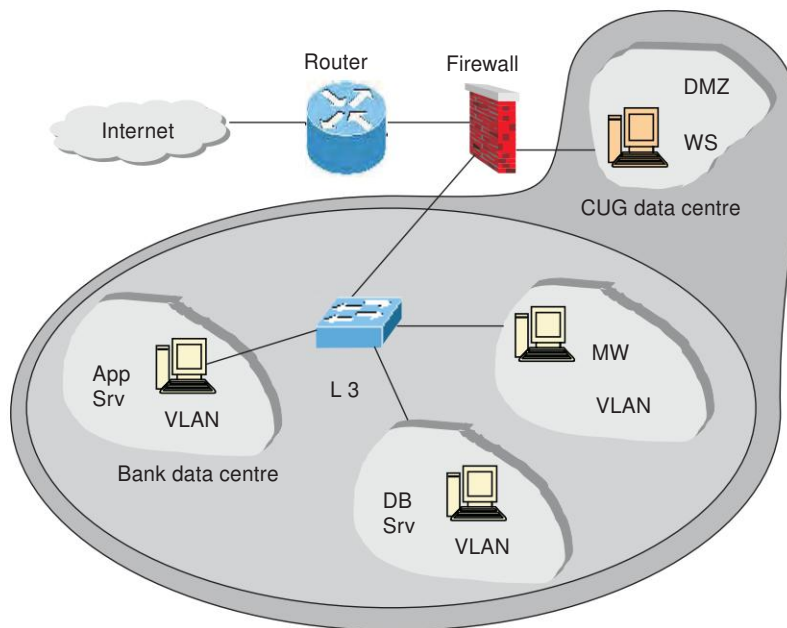


Fig. 7.11 Centralized environment: Internet banking architecture

In such a scenario, the advantages and disadvantages to the bank are, as given below:

- *Advantages:*
 - Reduced infrastructural costs
- *Disadvantages:*
 - Dependence on a third-party for all matters

Option 3: Bank has its Website, Hosted in a Third-party Data Centre, with a Shared Database

The following assumptions are made in this case:

- The database is centralized
- Single-platform application
- The bank may have its own WAN, but the Internet banking setup is hosted in the data centre of the TSP (Third-party Service Provider), with a shared database
- Web hosting at the data centre of the TSP, on a shared web server

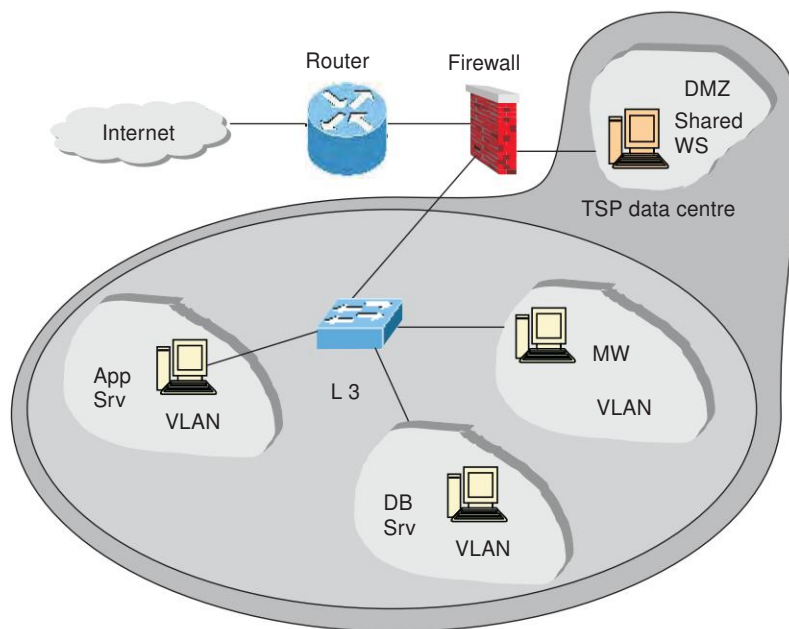


Fig. 7.12 Centralized Environment: Internet banking architecture

Box 7.1

Secured architecture: some tips

- Never let your network have multiple gateways to the Internet.
- Avoid using dial-up modems for connecting to the Internet, especially when the network has a secured channel for it.

(Contd)

- Never let your equipment vendor, design your infrastructure, without having a third-party review it. The third-party should preferably be vendor-neutral.
- Never assume that an architecture is functionally secure, even if it looks fairly good from a topological standpoint.
- You need to assess and probe the application, data and services, before you declare an architecture, 'fairly secure'.
- Security is a continuous process. This needs to be continuously assessed and improved upon.
- Complete security is a utopia, it can only be achieved at zero utility or at an infinite cost.

MULTI-LAYERED SECURITY MODEL

The multi-layered security model, is based on the premise that each financial transaction, uses multiple layers of security and every layer, adds a different technology, resulting in a trusted system that is monitored, at all times.

The components of this architecture and its arrangement in a security model are shown in the diagram below (pyramid):

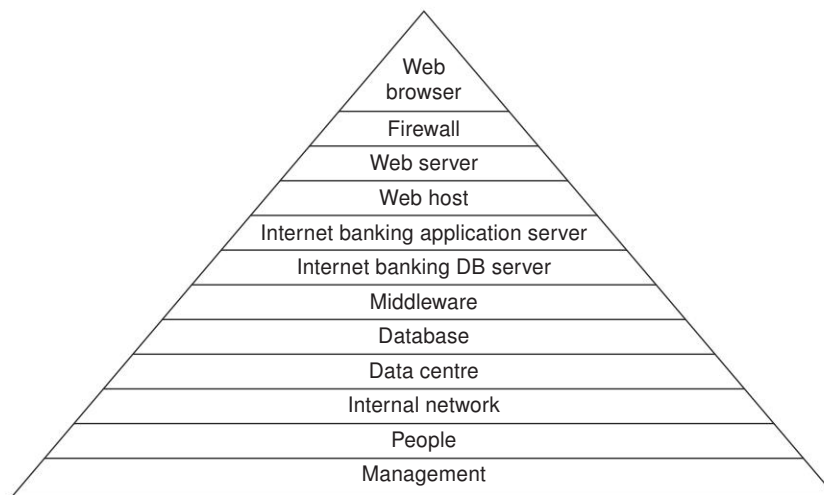


Fig. 7.13 Internet banking layered architecture

A multi-layered security model shows clearly, that the management 'layer' is the foundation on which, the entire architecture and its security, rest. The top most 'layer' or the layer at which the customer will operate, is the web

330 *Information System Audit and Assurance*

browser. For the sake of understanding, we will now see the function of each layer, starting from the top of the pyramid, and the risks and controls, associated with these layers.

It should be noted that the physical security of the entire system, should be ensured.

Web Browser

It is a software application that locates, loads and displays web pages, to the user.

Risks

- Browser crash
- System damage
- Lack of privacy
- Misuse of personal information

Controls

- Hide unnecessary information
- Customize error messages, to not reveal proprietary information
- Use robust logon methods and display exact information, without revealing unrelated information
- Avoid display of session IDs
- Implement timeouts, after a designated period of continued idleness
- Avoid 'history' option
- Use encryption mechanisms
- Avoid the use of 'cookies' and 'hidden fields'

Firewall

A system or a group of systems that prevents unauthorized access to or from the 'private' (trusted) network (the bank's own network, in this case), and sits on the perimeter of the private network and the Internet.

Risks

- System failure
- System compromise

- Misconfiguration
- Improper administration

Controls

- Ensure availability and redundancy of the system
- Determine the inbound and outbound access policy and apply correctly
- Monitor regularly, to ensure proper functioning

Web Server

A system that houses and delivers the web pages, to the web browser. It is at the bank's end.

Risks

- System failure
- Presence of unnecessary services
- Misconfiguration
- Multiple administrator-level access
- Not protected by the firewall
- Authentication of content

Controls

- Ensure availability and redundancy, through clustering and mirroring
- Place the web server in a network, protected (with bare minimum protection) by the firewall, viz. the DMZ
- Limit the number of administrator-equivalent access
- Remove or disable all the unnecessary services
- Limit the number of connections, to ensure normal speed
- Ensure proper and secure content management and uploading of content
- Install host-based IDS, to detect intrusions
- Ensure monitoring and auditing of the server
- Implement Public Key Infrastructure (PKI) for web server authentication

At this stage, we will deviate a little and explain 'Public Key Infrastructure' and other related areas.

PUBLIC KEY INFRASTRUCTURE (PKI)

Before discussing Public Key Infrastructure, let us understand the concept of, authentication of paper-based records and then, analyze the best way to replicate or improvise these, in an electronic record.

In case of paper-based record, the most, rather the only way of authenticating the record, is appending the signature of the person, who owns the contents of the document. If the document is official, we insist that the official seal of the organization be appended along with the signature of the concerned official. We also insist, that whenever there is any change/overwriting in the document, the same should again be authenticated, in exactly the same way as the original authentication, i.e. signature or signature with the organization's seal, etc.

Now, the question of verification of the signature arises. This can be done in many ways. In the *first* situation, the individual carries an authenticated document, with his/her specimen signature on it. The signature of the person is verified, by making the person sign, in the presence of the verifier. If the signatures match, in the view of the verifier, then authentication is complete, else, the document on which the specimen signature has been made is referred to the issuing authority. Examples of such verification are signing credit card charge slips, countersigning traveler's cheques, signing the immigration form, etc. The problems/issues involved, in such kind of verification are:

1. The person has to be physically present for signing the document, in the presence of the verifier
2. There is no accurate verification measure. Verification is consequently, dependant on the human eye or the capacity of the verifier to compare the signatures. This is based on the premise that most people cannot, spontaneously reproduce the signature of another person
3. Verifying the genuineness of the documents itself may be a problem, for example, verifying the genuineness of a traveler's cheque, etc.

The *second* type of situation is one, where the signed document is presented, in the absence of the person, whose signature it bears. This is just like the presentation of cheques to the bank, where the bank verifies signatures, from their signature sheet, which is maintained by the bank. The problems/ issues involved in such kind of verifications are:

1. The handling of the signature sheet
2. The signature in the sheet may not be current

3. Forgery of signature is comparatively easier, than when signing it in front of the verifier
4. Easier to trust the signature sheets, maintained by the bank
5. Even if the signatures match, a person can deny that the signature is his/her's and instead, may allege that the signature is forged. This is called repudiation

For all the above, let us see how we can ensure the confidentiality, integrity, authentication, and non-repudiation of the record.

Confidentiality, in the kind of environment discussed above, is protected by various administrative measures like, marking a record 'confidential', putting it in a sealed envelope, etc. *Integrity* is protected by *authentication* of any overwriting/cutting/modification, etc., by appending the signature, or signature and seals, wherever required. *Non-repudiation* is again, protected by the same signature, and related administrative measures. Problems of unauthorized access to the contents of the envelope and again sealing it, forgery of signatures, which cannot be distinguished by the naked eye, are not properly addressed by such kind of mechanisms/arrangements.

Now, let us see how such things can be handled in the electronic document. The functionality requirements for maintaining confidentiality, integrity, and non-repudiability, in an electronic document are:

1. The content of the document should be attributable to an owner
2. Any change in the content of the document, after the authentication of the owner, will become known to the user or beneficiary of the document
3. There is mechanism to ensure that the owner of the document, cannot deny having authenticated it

The following section will explain how the above functional requirements are implemented, using digital signatures and Public Key Infrastructure.

DIGITAL SIGNATURE

The Indian Information Technology Act, 2000, specifies that electronic records are to be authenticated solely, by the use of *digital signatures* which are based on *asymmetric crypto system* and *hash function*.

Digital signatures in this context, essentially mean, some kind of digital information, which is exclusive to the owner of the document and is affixed or attached to the document, for authentication. Now, the question is, how does the owner of the document, generate digital information? And how does this get linked with the document?

For understanding the above, we should have some basic knowledge about a hash function and asymmetric cryptography. A *hash function* is a value, which is created by taking different parameters, from the document. Let us take the following statement, as an example:

“IDRBT spearheads the technology absorption, in the banking industry.”

In this case, we can take a simple hash function to be, the number of times the letter ‘e’ appears in the statement, i.e. frequency distribution of ‘e’. The hash for the above statement then, is 5 (Five). Any change in the statement, which affects the frequency distribution of ‘e’, will change the hash value. This example has a very simple hash function, which is dependant on a single letter in the statement. But the hash function, used for a digital signature, is computed by taking various parameters of the documents. Hence, even a simple, miniscule change in the document/data, will affect the hash value. There are a number of industry standard functions available, which have properties that are desirable for a hash function. Some of these, are MD5, SHA, etc. As per the US National Institute for Standards and Technology (NIST), SHA is used as the hash function for digital signatures. It takes an electronic document of any size and produces a hash value that is 160 bits-long (decimal number of 50 digits). The design of the hash function is such, that the probability of two records, having the same hash value, is extremely low. So, at this stage, we assume that you have understood the basics of a hash function.

Now we will see, how this is used for a digital signature. In case of a digital signature, the first process is that of converting the document to a hash, using SHA, encrypting the hash, using the private key of the owner and then linking it to the document. We are aware that we have used certain words here, like, private key, which needs some explanation. *Private key* and *public key* are two ingredients of asymmetric cryptography, where, using some algorithm (RSA, as prescribed by the Indian IT Act, 2000), the owner will generate two keys, which are basically, two prime numbers, comprising 150 to 300 digits (512 bits to 1024 bits, in case of RSA). The private key, as the name implies, is totally private to the owner, whereas, the public key, is public.

Now, the data encrypted, using the private key, can be decrypted only by using the public key and vice versa. So now, it is clear that a digital signature is nothing but the encrypted hash function of the document. In order to verify a signature that is claimed to have been affixed by the owner of the document, the recipient has to decrypt the hash value, using the public key of the owner, which is publicly available and also has to compute the hash value of the document, using the same algorithm, say, SHA. The computed hash value is again compared with the decrypted hash value and if the two match,

then it is concluded that the document must have been signed by the claimant and that it has not been modified, enroute. In this way, the digital signature takes care of authenticity (signed by the claimant), integrity (not changed enroute) and non-repudiation (the owner cannot deny having signed it, as his/her private key has been used). Although digital signature has nothing to do with confidentiality, the owner can of course, enforce confidentiality, by encrypting the contents of the document, using the recipient's public key that only the recipient can open, with his/her private key.

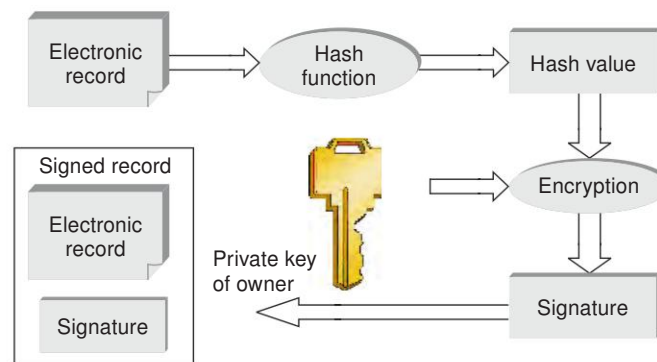


Fig. 7.14 Signing an electronic record

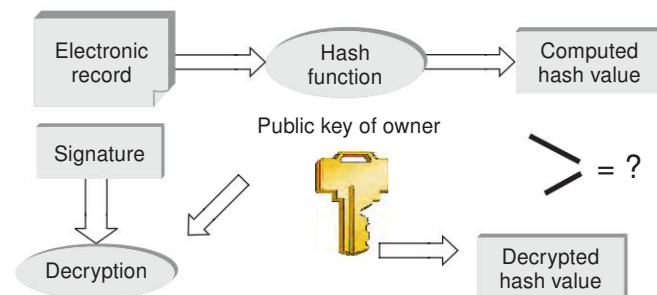


Fig. 7.15 Verifying a signed electronic record

Now, let us discuss the security aspect of a digital signature. There are broadly three aspects of security in this context. One is the security of the digital signature itself, i.e. where should it be stored, etc., the second is that the hash value should not be the same for two different records and the last, is deducing (computing) the private key from the public key.

In case of the first, the options available, for storing the private key include, are hard disk, smart card, I-Key, Hardware Security Module (HSM), etc. The

various risks and controls, over storage of the private keys, in all these options, are however, not within the scope of our discussion. Yet it is important to mention that it is always advisable, to store the private key with another symmetric encryption and keep the private key out of the hard disk of the computer. The key, for symmetric encryption, should be remembered by the users. As regards the choice for keeping it outside the hard disk, one can alternatively use either the smart card, or I-key, or HSM, or HSM with I-key. In all these cases, the key-generation and storage will happen in the device itself.

The next point, is the uniqueness of the hash value, i.e. whether or not, the hash value can be the same for two different records. Although, it is possible for two records to have the same hash value, such a possibility becomes remote, if we use a reputed algorithm, like, SHA.

The next issue is that of the uniqueness of the private key. Since the key pair in the asymmetric cryptosystem is generated randomly, there is a very remote chance of the key being duplicated. But to ascertain whether a key is duplicated or not, you need to compare the public key with all the other, genuine public keys, available. The above discussion makes it clear that the digital signature, generated, using asymmetric cryptography, is fairly secure.

Now, let us consider a situation, where an entity 'A' prepares a message for 'B' and digitally signs it. Before 'B' receives the message, let us say, another entity 'C', intercepts the message, changes its content and again signs the message, using its (C's) private key and sends it to 'B', as 'A'. Now when B receives the message and tries to verify the digital signature of A, he/she will naturally need A's the public key of A to decrypt the hash. At this stage, C again intercepts the communication and makes available, his/her own public key, instead of A's public key. Now, the hash gets decrypted and it tallies with the new hash, generated by A and there is no reason to disbelieve that the message has been sent by A and has not be changed enroute. The success of this scheme is of course possible if C is able to intercept all the communication that emanates from A and travels to B, which is not at all impossible.

Now, if you analyze the above situation, you will realize that the problem is not the security of the private key, but the authenticity of the public key, which created such a situation. The recipient 'C' had to believe the name-public key association, which he/she received. In other words, when 'A' received the public key, he/she believed that the key belonged to B, when actually it belonged to the interceptor, i.e. 'C'. How does one deal with such a situation?

For this, you probably need to give a little importance to the public key. While receiving the public key, you need to be doubly sure that the public key belongs to the owner of the document, who had put the digital signature. The

solution to all these problems is the “Public Key Infrastructure (PKI)”– a trust infrastructure that consists of:

- An organization that issues a digital certificate, called ‘certifying authority’
- A method of storing and publishing digital certificates and Certificate Revocation List (CRL)
- Technical, operational, and managerial procedures, concerned with issuing and managing digital certificates (certificates for the public key)
- Well-defined ways for applications to use digital certificates
- Support for inter-operation, among different certification authorities

IDRBT is the one of the certifying authorities, as per the Indian IT Act, 2000 and the details of this, can be viewed in the Certificate Policy Statement (CPS), available at <http://www.idrbtca.org.in>.

Box 7.2

Phishing—The new menace for Internet banking

Who wouldn’t be worried by an E-Mail from their bank, saying that their account had possibly been compromised and that they need to confirm their details and password to ensure continued access? Upon receiving such an E-Mail, most of us would probably race to respond as quickly as possible.

Yet the chances are that in doing so, we wouldn’t be helping anyone other than the criminal who wrote the E-Mail. Creating false E-Mails that pretended to be from a bank or other authority, but which are actually designed to collect sensitive information, such as passwords, and then use them for fraudulent purposes, is the latest problem to dog Internet users—a phenomenon known as “Phishing”. (The name reflects that fact that such E-Mails are “fishing” for information.)

As well as attempting to collect passwords and other sensitive data, many phishing messages also attempt to install spyware, Trojans (allowing hackers to gain “back door” access to your computer), or other nasties. Even collecting passwords can be dangerous—after all, once they have your account number and password, hackers can easily transfer money from your account to any other location.

Some phishing mails ask for a response by E-Mail; others include a form to collect details, or include a link to a website that resembles the actual site you expect to visit, but is actually a clever clone. Like spam,

(Contd)

phishing mails are sent to the widest possible audience, so it isn't unusual to receive a message asking you to confirm account details for a bank you don't actually deal with. Phishers rely on the fact that even if 99 per cent of recipients ignore an E-Mail, 1 per cent are likely to respond.

So be aware of fraudulent E-Mails, particularly those related to Internet banking.

We started this discussion, in the context of authenticating a browser with a web server. Let us first understand why we need browser and web server authentication? For example, if you logon to some Internet banking site, by entering the URL, viz. www.abcbankonline.com in the browser, you are likely to get content from the web server of "abc bank". But how can we be sure, that the contents are not spoofed and that you have received content, which only looks like content from bank's web server? In case the bank's site is spoofed, the credentials that you enter, for authentication, i.e. user ID and password, maybe captured by the perpetrator, who can then, immediately go to the actual site and perform some transactions, using your credentials, which he/she captured earlier. To prevent such occurrences, you need to have a two-way authentication procedure, between the browser and the server. This can be achieved by implementing PKI, where the server and the client, get authenticated between themselves, before sharing the resources. The Secure Sockets Layer (SSL) protocol, originally developed by Netscape, has become the universal standard on the Web, for authenticating websites, to the web browser users, and is also used for encrypting communications, between browser users and web servers. Since SSL is built into all major browsers and web servers, simply installing a digital certificate or server ID, will enable SSL capabilities. The SSL handshake procedures, which help in authentication and maintenance of confidentiality of data, between the server and the browser, are as follows:

1. The customer's web browser sends the website server, its methods of encrypting data. This includes, the encryption type, some random data that the encryption programs on both sides can use in the scrambling routines, and other SSL-related data like, the SSL version number, etc.
2. The server returns its own random data, to be used for encryption and also, its SSL certificate. This certificate is nothing, but the public key of the server, certified by a Certified Authority (CA). The certificate of the certificated authority means, putting the digital signature of the CA, on the public key of the server. Though the SSL certificate is bound to the fully-qualified domain name, the

web servers, link the certificate to the IP address. The result is that, if you attempt to have more than one SSL certificate, associated with the same IP address (in the case of virtual hosting), you may get undesired results.

Typically, the certificate that will be used for the IP address, no matter which domain you attempt to access, will be the first one, in the web server's configuration file. This information is important for a website owner, because many of the budget and free web-hosting services do not give you, your own IP address. Getting a unique IP address for an SSL certificate is usually, the main factor that leads to extra-pricing for secure hosting on the budget web hosts, and can often increase your pricing, beyond that of a full service host. Even with full service web hosts, if you need separate certificates for multiple domains, you will often need to open individual accounts for each, so that they have their own IP addresses. On the other hand, since the certificate itself, is not linked to the IP address, you can usually move the certificate from one web host to another (as long as you have a unique IP address, at the new host).

3. The customer's browser, checks the information it receives and compares it with the domain with which, it was trying to securely connect. If the secure certificate information on the website, does not match the domain name, the browser will notify the customer that there is a problem. The certificate expiration date and valid certificate authority are also checked, at this point.

Box 7.3

The unending trust

For checking the authenticity of the certificate authority, the browser needs to have the certified public key of the CA. Some of the certificates, come bundled with the browser software, where there is no need for importing the certificate from other sources. But in such cases, there is an implicit trust on the certificate provider, which may not be acceptable to the user, who needs the certificate from a trusted third-party, whose certificate may not be bundled with the browser software. In these cases, you need to import such a certificate, by securely logging into the website of the CA. Here the problem of checking the authenticity of the CA again arises and the problem never really ends. At certain points, you need to have explicit trust on either the CA or the root CA. Imagine, in case of

(Contd)

Internet banking, if the banker, while providing the user ID and password for Internet banking users, also provides a server certificate and the certified public key of the CA, to the user. Will the problem related trust, reduce, even a little? We think it would for we at least trust our banker!!

4. The browser, now creates a “premaster secret” that will be used to encrypt the rest of the session. This is a random key that it encrypts, using the encryption method agreed upon and combines it with the server’s public key string that it received and sends the new encrypted secret string, back to the server. If the server requires client authentication, it is done at this point, using the same steps as described above.
5. With the new “premaster secret” string, both, the browser and the website server, create a new “master secret” string and use it to create session keys (long strings of generated characters) that their encryption programs use, for the rest of the session, to scramble and unscramble (encrypt/decrypt) all transmissions, for the rest of the session. With the master secret key in place, both sides are also able to verify that the data wasn’t changed enroute.
6. The browser, now has the information it needs, to establish secure communication and it sends a message to the server, saying that it will start using the new session key.
7. The browser (now talking in the encrypted format) verifies to the web server that it is finished, locking/securing its part of the session.
8. The web server then sends a message to the browser, saying that it too will start using the new session key.
9. The web server (now talking in the encrypted format) verifies to the browser that it is finished, locking/securing its part of the session.

The remainder of the SSL session, gets processed between the browser and the web server, using the encryption, agreed upon with the master secret phrase as the key.

Web Host

It is the operating system (OS) on which the web server software works.

Risks

- Unrestricted access to users

- Unknown and unnecessary services on the OS
- Loopholes, like, missing updates and patches

Controls

- Ensure capacity planning and monitoring of CPU, memory and disk resources
- Ensure logical file separations of documents, related to the website and ensure proper user access rights on those files and folders (at the system level)
- Never display or disclose information, that is not necessary, to the users of the website
- Remove or disable all the unnecessary services
- Use a dedicated system for hosting the web server
- Install updates and patches on the system, after proper verification and testing

Internet Banking Application Server (IBAS)

It is the system on which the IB application resides.

Risks

- System failure
- Unrestricted insider-access
- Poorly configured OS

Controls

- Ensure availability and redundancy, through clustering
- Place the system in a logical subnet, with proper user-access controls and rights
- Remove or disable all the unnecessary services
- Ensure physical security
- Ensure regular backups

Internet Banking DB Server (IBDS)

It is the system on which, the details and information of each Internet banking customer, is stored.

342 *Information System Audit and Assurance*

- This layer has the same risks and controls as the preceding layer (IBAS)
- It should be ensured that no alterations/modifications can be made to the 'live' data by anybody with access privileges to the system, at the system level
- Ensure regular backups

Middleware

This convert data between the IBDS and the database to a standardized format

- In the case of centralized solution, the database is centralized and the connection between the middleware and the database, should be through a firewall
- In the case of distributed solution, the database and the middleware would, in most cases, be on the same LAN. The least, the bank can do is to put the two systems in two separate VLANs and ensure proper access controls and rights

Database

This system contains the entire information and details about the entire core bank business. This could be centralized or distributed.

Risks

- Poor database design
- Tampering/loss of data

Controls

- Database configuration should be proper and, preferably, one-time
- Only tuning of the database should be a continuous process
- Ensure proper user-access controls and rights, to avoid tampering with data, by unauthorized users
- Ensure regular backups

Data Center

A data centre is a large data-housing infrastructure, that provides secure, high bandwidth access to clients, for a range of network (Internet, in this case)

related services. Essentially, it comprises servers, firewalls, high bandwidth network (Internet) links, and stringent physical security facilities.

Risks

- Physical security
- Access security

Controls

- Round-the-clock monitoring
- Physical access control mechanisms like, access card, PIN, biometrics, etc.
- Environmental protection from water, fire, power surges, etc.
- Ensure access, only to authorized persons, using any of the mechanisms mentioned above,
- Logical access controls on systems, residing in the data centre like, lock-out, password-protected screen savers, etc.

Internal Network

A group of systems linked together, to form a network, generally, the LAN of the bank at the data centre. Some of the 'layers' mentioned above, may have direct physical connectivity with the Internal network.

Risks

- Unauthorized access to network resources
- Poor maintenance of network

Controls

- Limit usage of resources, to authorized personnel only
- Use any of the access control mechanisms, to ensure restricted access.
- Maintain and monitor all the system resources

People

The human resource, present in the data center, who are involved in the operations. Generally, 'people' include, system administrators, network

344 *Information System Audit and Assurance*

administrators, database administrators, security administrators, and other personnel, involved in the operations. Their responsibilities include:

- System installation, configuration, management, and maintenance
- Ensuring proper access control rights, maintaining and monitoring logs, and enabling system auditing
- Ensuring proper backups of all systems

Risk

- Social engineering

Controls

- 'People' should not divulge confidential information to any outsider
- 'People' should not discuss confidential information in public
- 'People' should not divulge their user IDs/passwords to anyone, under any circumstance

Management

This 'layer' is the top-level management of the bank, that has chosen to incorporate IB, as one of its delivery channels.

- This 'layer' should do the initial study on the ROI and feasibility of choosing IB delivery channel
- Their responsibilities include, carrying out capacity planning and estimation; ensuring that proper policies and procedures are in place, like Business Continuity Plan, Disaster Recovery Plan, other contingency plans, etc.
- Ensure that all regulatory and supervisory issues are complied with

BASICS OF PENETRATION TESTING

What is Penetration Testing?

- This is a process of assessing the security of the network, host, and applications
- Network penetration testing, in a nutshell, consists of a team of security specialists, trying to compromise the security mechanism, protecting your network, either through the Internet, by working

from within your enterprise, through dial-in, through partner-connect or sometimes, even using social engineering techniques

- In case of host penetration, the servers and other host systems are assessed for known vulnerabilities in the operating systems and server applications
- The penetration testing of the application is aimed at finding, known vulnerabilities in the business applications and database management system

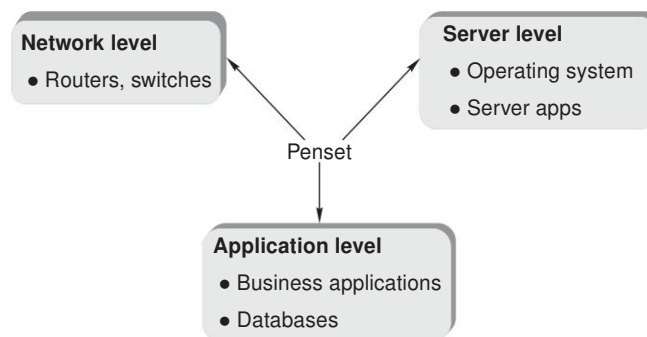


Fig. 7.16 Penetration test

The Scope of Penetration Testing

Whatever we have discussed above, is basically a security assessment of the network, servers, hosts, and applications. But why do we call it penetration testing?

Why Do We Call it Penetration Testing?

- In all these above-cases, an attempt is made by a group of security professionals to expose the vulnerabilities to the management, but not to anyone else
- For exposing the vulnerabilities, the security professionals need to conduct an “ethical hacking” operation or penetration of the infrastructure, with the permission of the management
- In case of penetration testing, the security experts should know where to stop. Otherwise, instead of exposing the vulnerabilities to the management, they will exploit the vulnerabilities, which would cause a material loss to the assets

What are the Questions that are Answered by Penetration Testing?

- How much critical information is revealed to outsiders/users?
- What are the access weaknesses, from the outside?
- What is the extent of traversal, possible from the perimeter?
- What attacks are likely to materialize, from outside?
- What will be the extent of material damage?

What Do We Get at the End of the Penetration Test?

Although the penetration test report could vary across the organization, as per the charter and engagement letter, still, there are some basic things, which should form part of the report, viz.:

- A report, detailing vulnerabilities found, means of exploitation, risk level (ease of exploitation/extent of damage), etc.
- Details of tests carried out and their results
- Mitigating the options for weaknesses
- Sample exploits, if required

Flavors of Penetration Testing

Vulnerability Scanning

In case of vulnerability scanning, some automated tools are run, which scan the hosts in the network and check them for a set of, known vulnerabilities in well-known services or operating systems. The purpose and value of this scan, is to find out whether someone has installed a new server or host or has opened up a service, that should not have been opened, as per the business decision or documented security procedure. This will also help, find, glaring problems in implementation, such as, implementing a Windows server in an out-of-the-box configuration and not applying any service pack.

Vulnerability Testing

Vulnerability testing is like vulnerability scanning, except that, in the case of testing, automated commercial scanners are run for a particular IP address, to find out known vulnerabilities. One thing, which is very important from a control perspective is the authenticity and reliability of the scanner. The way threats are growing, the updates to the scanner should also be commensurate

with new threats. Otherwise, running such a scanner can only protect you from “script kiddies” hackers, who download pre-canned attacks from the Internet, rather than probing and prodding your networks, over weeks or even months.

Red-team Penetration Testing

Red-team penetration testing, is the highest level of network assessment, where a team of skilled security practitioners (red-team), attempts to exploit the vulnerabilities in your network, the same way that a determined and a skilled hacker would. The red teams are like marines. They adapt, improvise, and overcome. A comparison between scanner and red team assessment would make the point clear.

Let us take the example of the “msadc.dll” vulnerability. This vulnerability can exist, only if the following conditions exist:

1. The target web server is running a Windows operating system
2. Msadc.dll is present and accessible on the target server
3. The target server is running IIS 4.0
4. A set of file associations exist, on the target server
5. Appropriate data sources exist, on the target server

Now, let us take two cases. In one, the msadc.dll file is present, but not in the default location and all the other conditions exist. In another case, the msdc.dll is present in the default location, but all the other conditions do not exist. In the first case, the security scanner will not find the file in the default location and will conclude that the vulnerability does not exist, whereas the vulnerability actually exists. In the second case, by finding the file at the default location, it will conclude that a vulnerability exists, whereas there is actually, no vulnerability. The file at the default location, could be a honey pot for reaching out to the perpetrator or hacker. In case of the red team, it does not stop, whether or not it finds the file in the default location. It knows that sometimes, administrators try to design security by obscurity. It searches all the locations and takes a decision, depending on all the components, which are necessary to trigger an attack.

AUDITING INTERNET BANKING

Usually, a complete Internet banking audit, has the following components, viz.:

1. Management control review, pertaining to Internet banking, which consists of issues relating to strategy, outsourcing, training, etc.

348 *Information System Audit and Assurance*

2. Application control review of the Internet banking application, which comprises the application and also, the related services, viz. Web server, Web host, etc.
3. Network control
4. Penetration testing

The following is a checklist for Internet banking audit. Although care has been taken to include important issues, pertaining to the above components, yet this alone, will not suffice for conducting a full penetration testing operation. The application control aspect of the checklists, can also be used for auditing any web-based application. This checklist can also be used by the security administrator, for implementing appropriate security measures.

INTERNET BANKING AUDIT CHECKLIST

Management related issues score

1 = Poor, 2 = Not clear, 3 = Needs Improvement, 4 = Satisfactory

No.	Particulars	1	2	3	4
1.	Strategy Is there a business, marketing, and technology strategy? Has its feasibility been assessed? Have goals, success factors and Return On Investment been assessed? Are delivery timescales realistic?				
2.	Security management Is there a security policy, duly approved by the board of directors? Is there segregation of duty of Security Officer/ Group, dealing exclusively with Information Systems security, and the Information Technology division which actually implements the computer systems? Is the role of the Information Security Officer independent in nature? Is the role of an Information System auditor independent in nature? (It should be independent of the Operations and Technology unit) Bank should ensure that Information Systems auditor forms part of their internal audit team.				
3.	Service level agreement Have Service Level Agreements been produced, detailing: • Availability				

(Contd)

No.	Particulars	1	2	3	4
	• Time to fix • Time to implement changes • Backups • Volume-based throughput • Security • Right to audit • Minimum level of services				
4.	Training Has a security awareness training and education program, been implemented?				
5.	Has a capacity monitoring process, been implemented? Establish an overall capacity planning process for Internet banking websites, observing the following principles: • Ensure that hardware platforms and communication links are readily scaleable, to respond to increases in demand, without fundamental changes in architecture • Establish monitoring processes, to measure use of the physical resources and communications bandwidth, so that upgrades can be arranged, before capacity overloads become problematic				
6.	Are potential security problems identified? Identify sources of information on new security vulnerabilities, in the technology being utilized, for example, CERT, SANS and other mailing lists, supplier websites • Establish a workable and reliable change control process, with event logging and reporting procedures, to ensure that updates are made in a safe and timely manner • Monitor the list of the currently available service packs and hot-fixes, on the websites of product vendors, to ensure that the most recent versions are in use • Test hot-fixes before installation • Install hot-fixes in the correct order				
7.	Are changes managed effectively (hardware, software and content)? • Document the change management process and ensure that its scope is clearly understood				

(Contd)

No.	Particulars	1	2	3	4
	• Establish a formal mechanism for identifying the security impact of changes and ensure that this is evaluated by a qualified individual • Implement an approval process, clearly identifying the sign-offs required, for changes to take place • Record all controlled changes, in a comprehensive and consistent manner • Ensure that contingency plans are prepared				
8.	Is security monitored? Conduct regular and frequent checks, to ensure that website components continue to adhere to the agreed configuration standards, required for security • Carry out a 'baseline review', before a website is initially connected to the Internet and compare subsequent reviews with this baseline, to detect changes • Check that the website components are not vulnerable to newly-emerging threats • Conduct active 'penetration' testing, to simulate external attacks on websites • Use automated tools, to support monitoring, wherever possible				
9.	Is an effective logging process implemented? Develop an audit/event logging procedure that preserves the integrity of logs, by taking the following points into consideration: • Routinely backup all logs, to a directly attached device • Keep logs (and spool directories) on dedicated disk partitions, to reduce the effect, of them filling up the rest of the system • Use drop-safe logging, where the audit/event records are transmitted from the host to a dedicated PC, via a serial link, or to protected media, such as, a WORM disk • Determine what action should be taken when the capacity of the logs has been reached, for example, • Schedule frequent checks of disk usage, and automatically page the administrator, when the device is approximately, 90 per cent full.				

(Contd)

No.	Particulars	1	2	3	4
	<i>In extreme cases, it may be desirable to halt the entire system, to avoid unlogged activity. However, this action will make the system vulnerable to deliberate denial of service attacks.</i>				
10.	Is appropriate information logged?(Audit Trail Control) • Log-on and log-off success and failure • Restart, shutdown and system success and failure • Security policy changes: success and failure • User and group management success and failure • File and object access success and failure • Use of user rights success and failure • Departures from 'normal' usage patterns such as: • System load at different times of the day • Number of processes running • CPU utilization • Unusual successes/ denials of connections • Success and error messages from both firewalls • Multiple access attempts • Access to unusual ports.				
11.	Is intrusion-detection, implemented? Implement an intrusion detection process, adopting the following principles: • Use a respected commercial package that is regularly updated, to keep up with new vulnerabilities and attacks • Keep the intrusion-detection tool up-to-date, by applying the latest patches and attack signatures • Run the absolute minimum of services, on the platform, hosting the intrusion-detection tool • Do not allow the platform's interface to be visible to the perimeter networks, being monitored • Establish an administration and reporting network for the intrusion-detection system that is isolated from the internal network • Do not rely extensively on the intrusion-detection tool and ensure that other security procedures are in place				

(Contd)

No.	Particulars	1	2	3	4
12.	Is incident management implemented? Implement an effective process for dealing with security incidents. This could be based on the following six steps: 1. <i>Prepare</i>: Develop and document the response plan and identify the staff, tools and external resources that may be required. 2. <i>React</i>: Put the plan into action, by assessing the severity of the incident and establishing management control. 3. <i>Respond</i>: Gather the appropriate resources, to tackle the incident and gather information. 4. <i>Contain</i>: Identify and remove the cause of the incident and improve defences. 5. <i>Recover</i>: Restore the system (from backup, if necessary) and verify that vulnerabilities have been removed. 6. <i>Follow-up</i>: Review controls in the light of the incident and confirm the effectiveness of incident-detection and response processes.				
13.	Is adequate support provided? Ensure that adequate resources are in place, to support the incident management plan. These are likely to include: • Incident-response team leaders and team members, with high levels of technical skills • Ready access to external agencies, for backup support • Readily available hardware and software for incident investigation • Training courses, checklists, guidelines and procedures				

OUTSOURCING ISSUES

Although few banking organizations maintain their Internet banking web servers, in their own data centers, outsourcing is an approach that is today, commonly adopted for web servers, often, because of a lack of appropriate technical skills, within the organization. The options available, for outsourcing web hosting, include:

Box 7.4

Own machine on provider network.

This model is referred to as server co-location. The owner is responsible for providing a fully-configured web server, which is located in the service provider's facility, with a high-speed connection to the Internet.

Rent space on shared machine, on provider network.

Many providers offer the service of rented disk space, on a shared website, for a monthly fee. Individual renters are only responsible for ensuring that the information is accessible from the Internet. This is common for small companies, where the equipment and skills, required for a dedicated website cannot be justified. (This is not suggested for hosting Internet banking website.)

Organizations contemplating outsourcing of websites, should give consideration to how the following issues will be addressed and, where necessary, contractually agreed upon:

- Establishing security targets and linkage to a risk/reward policy
- Identifying how security monitoring will be conducted and reported
- Assessing the security of the third-party's network architecture
- Assessing the third-party organization's security practices and culture
- Identifying the third-party's ability to respond to new vulnerabilities
- Identifying the third-party's ability to respond to security incidents
- Identifying data backup and disaster recovery requirements
- Implementing secure mechanisms for remotely updating website content
- Establishing the right to conduct security tests and reviews.

Web-based applications— Audit checklist score

1 = Poor, 2 = Not clear, 3 = Needs Improvement, 4 = Satisfactory

No.	Particulars	1	2	3	4
1.	Is unnecessary disclosure of information, avoided? Review the source of HTML, JavaScript and other client-side scripting languages, to ensure that these do not contain unnecessary information that could be noticed and exploited by potential attackers. This might include:				

(Contd)

No.	Particulars	1	2	3	4
	• Developer names (could be used for social engineering) • Disabled functionality • Details about Common Gateway Interface (CGI) functions and parameters • Third-party tools in use, which may be vulnerable Review error messages, returned by the web-based application, to ensure that they do not reveal undesirable information.				
2.	Has a robust logon process been implemented? Where a web-based application requires users to log on, to authenticate themselves, consider the following factors in designing the process: • Logon failure messages should not indicate which of the username/password pairs submitted, was incorrect • Where http basic authentication is used, there is no account lockout after successive failed attempts and applications may therefore, be vulnerable to brute force attacks • Where account lockout is implemented, further logon failure messages should be carefully designed (for example, to avoid revealing when the password has been guessed correctly, even though the account is locked) • Avoid allocating system resources for a potential user session, before authentication is complete, thus, reducing the scope of denial of service attacks, based on initiating many logon attempts				
3.	Are sessions appropriately tracked? Web-based applications often need to implement mechanisms, to track transactions, within a user session, as the underlying http protocol cannot do this (it is stateless). When these mechanisms are designed, the following factors should be taken into account, to minimize the risk of the sessions being hijacked or cloned: • Avoid using mechanisms that can lead to session IDs being unnecessarily disclosed, See, for example, the sections covering GET/POST and Cookies below • Avoid session IDs that are easily predicted, by including a random element.				

(Contd)

No.	Particulars	1	2	3	4
4.	Are session timeouts implemented? Implement session timeouts for web-based applications, after designated periods of inactivity, if there is a likely risk, due to access to unattended browsers.				
5.	Are sessions encrypted, where required? Consider using secure session protocols such as, SSL to encrypt sessions, between browsers and the web server, to prevent sensitive application data from being intercepted.				
6.	Are GET/POST operations carefully implemented? Use http POST, rather than GET operations, to obtain information from users that may be sensitive, personal or that may compromise the security of the application. URLs requested by GET operations, are stored in the browser's history file and can also be passed on to other web servers, via the http Referrer field. This can lead to the disclosure of sensitive information. For example, the following GET operation could cause damaging information to be stored, in insecure log files: http://www.anybank.com/scripts/login.cgi?username=john&password=partyhat"				
7.	Are hidden form fields restricted? Avoid using HTML hidden form fields, to pass important or sensitive parameters from browsers to web servers. These fields, although not displayed in web pages, can easily be viewed by users (by viewing the HTML source) and modified, to cause unexpected results. An example of the use of hidden form fields, to avoid this, shown below: <INPUT TYPE="hidden" NAME="username" VALUE="harrisj"> <INPUT TYPE="hidden" NAME="password" VALUE="bank123e "> <INPUT TYPE="hidden" NAME="adminflag" VALUE="no">				
8.	Are cookies carefully controlled? Where cookies are used to pass important or sensitive information between the browser and web application, make sure that the cookie parameters are set to avoid, unnecessary disclosure of information.				

(Contd)

No.	Particulars	1	2	3	4														
	The structure of a cookie is shown below: <table><thead><tr><th>PARAMETER</th><th>MEANING</th></tr></thead><tbody><tr><td>NAME</td><td>Arbitrary string, used to identify the cookie, since a web server can send the user, more than one cookie.</td></tr><tr><td>DOMAIN</td><td>The range of hosts, where the browser is permitted to transmit the cookie.</td></tr><tr><td>PATH</td><td>The range of URLs, where the browser is permitted to transmit the cookie.</td></tr><tr><td>EXPIRES</td><td>When the browser must no longer store the cookie.</td></tr><tr><td>SECURE</td><td>Boolean value that indicates if the browser may send, only the cookie, over an encrypted session.</td></tr><tr><td>DATA</td><td>Arbitrary strings of text.</td></tr></tbody></table> Users can examine the contents of cookies, stored on their PCs. Even those which expire, at the end of the session, can be viewed by typing: JavaScript:alert(document.cookie), in the browser URL field. Some users prevent their browsers from accepting cookies, causing problems for the applications that depend on them.	PARAMETER	MEANING	NAME	Arbitrary string, used to identify the cookie, since a web server can send the user, more than one cookie.	DOMAIN	The range of hosts, where the browser is permitted to transmit the cookie.	PATH	The range of URLs, where the browser is permitted to transmit the cookie.	EXPIRES	When the browser must no longer store the cookie.	SECURE	Boolean value that indicates if the browser may send, only the cookie, over an encrypted session.	DATA	Arbitrary strings of text.				
PARAMETER	MEANING																		
NAME	Arbitrary string, used to identify the cookie, since a web server can send the user, more than one cookie.																		
DOMAIN	The range of hosts, where the browser is permitted to transmit the cookie.																		
PATH	The range of URLs, where the browser is permitted to transmit the cookie.																		
EXPIRES	When the browser must no longer store the cookie.																		
SECURE	Boolean value that indicates if the browser may send, only the cookie, over an encrypted session.																		
DATA	Arbitrary strings of text.																		
9.	Is user input validated? Validate data, returned from browsers, to check for unexpected values that could cause the application to behave in unintended ways. Particular things to check, include: • Values falling outside allowed ranges • Volume of data returned outside expected ranges • Special characters that could be misinterpreted by the application, for example: • %0A new line character (in hex) • pipe • ; semicolon • “ double quote • ‘ single quote • <% %> VBScript terminators																		

(Contd)

No.	Particulars	1	2	3	4
10.	Do not rely on client-side filtering of user input, for example, using JavaScript, as this can be circumvented by the user. Are scripts carefully constructed? Common Gateway Interface (CGI) scripts are used by web-based applications, to communicate with resources, such as backend systems and internal databases. They are prone to subversion and are a primary target of attackers. The following measures are recommended: • Store all CGI scripts in a single, separate directory, for example, cgi-bin, under the web server home directory • Allow only authorized administrators to access these • Do not include any command processors or interpreters, such as, Perl or command.com in the CGI directory • Validate all client-side input, to CGI scripts • Check for potential vulnerabilities in all CGI scripts, using tools, such as: • CGI Wrap (to force scripts to run as users, not as the web server owner) • TaintPerl (to prevent passing of unchecked input to system calls) • phf and Latro exploit test programs • Allocate sufficient memory for CGI scripts, to minimize the likelihood of a buffer overflow • Ensure that CGI scripts record a log of what they have done • Avoid using SUID shell scripts within UNIX • Use APIs or compiled programs, where possible, and test them thoroughly or use existing, tried and tested codes • Scripts should only be written by experienced script programmers				
11.	(a) Has security of the application, web server and web host been checked, before going into production? (b) Are scripts thoroughly tested to avoid subversion, including attacks, using buffer overflow techniques and embedded commands?				

(Contd)

No.	Particulars	1	2	3	4
	(c) Do scripts that allow users to send mail, only use secure mail programs, e.g. /usr/lib/sendmail and not /bin/mailx or /usr/ucb/mail? (d) Are 'forms' avoided, as any script can be called for directly, by entering its URL, with an embedded list of parameters? (e) Are Microsoft ISAPI scripts, only held in 'execute only' directories that web users cannot read or modify? (f) Have correct access permissions been set on web directories and on the pages and scripts they contain?				
12.	Is the application architecture secure? (a) Does backend connection to a database, avoid the use of privileged user IDs? (b) Does connection to a database, avoid the use of hard-coded passwords? Or • Are any hard-coded passwords held in obscure places? • Are hard-coded passwords lengthy and cryptic? • Are hard-coded passwords held, and on files are they adequately protected? (c) Is the web server run on a server, physically different from the backend application server? (d) Is sensitive customer data, (i.e. credit card detail) encrypted? (e) Are users prevented from calling backend objects, directly, e.g. by allocation of session ID, following successful login and encryption of link, between web server and backend data server?				

WEB SERVER SOFTWARE

Organizations have a wide choice of web server products, ranging from commercial offerings such as, Microsoft's IIS and Netscape's Enterprise Server (SUN iPlanet), to public domain or 'open source' products such as, Apache. Different web servers, have different security features and these should be considered, in selecting an appropriate product. However, other factors will have a major influence on the choice of the web server software such as:

- Choice of web host, for example, UNIX or Windows NT,
- Cost of purchase and support,
- Skills and experience within the organization.

Web server software— audit checklist score

1 = Poor, 2 = Not clear, 3 = Needs Improvement, 4 = Satisfactory

No.	Particulars	1	2	3	4
1.	Is unnecessary disclosure of information, avoided? Avoid, unnecessarily providing potential attackers, with information that could help them to find weaknesses in websites: (a) Suppress, if possible, the server field in HTTP headers, that identifies the web server's brand and version. (b) Ensure that directories of files, on the web server, are not indexable, as this can reveal the presence of files, not intended to be publicly accessible. (c) Ensure that the source code, of server-side executables and scripts, for example, CGI scripts and ASP files, cannot be viewed via, a web browser. (d) Are web servers, containing sensitive pages, run on alternate ports and is access restricted by the packet filter? (e) Has any sensitive information been removed from public web servers? (f) Are sensitive pages, secured by passwords or an access list?				
2.	Have known, server bugs been removed? (a) Ensure that the web server software in use, incorporates vendor-issued updates and patches, to remove known security problems. (b) Ensure that a process to receive notification, of any newly detected security vulnerabilities in the web server software, is in place, so that risks can be understood and managed <i>Vendors' websites, can be a good source of information on security problems that have been fixed, but may not provide any notification of known, but unresolved problems. Internet news groups and mailing lists, will usually, provide the most current information.</i>				
3.	Are users appropriately authenticated? Consider employing user authentication, supported by all web servers, to control access to specific web pages. The main options for implementing user authentication, are outlined in Table 7.2				

Table 7.2 Authentication mechanism in web server

	<i>Advantages</i>	<i>Disadvantages</i>
Basic Authentication Mechanism— based on simple username/ password.	Supported by all web servers and browsers, as a standard feature of HTTP. Well-understood by users.	Traditional disadvantages of fixed password schemes: Passwords may be easily guessable. Administrative impact of users forgetting passwords: Passwords in clear, on the Internet.
NT challenge/ response	Employs encrypted challenge/ response, to avoid passwords in clear. Suitable for intranets, where types are controllable.	Only supported by Microsoft IE browsers.
Certificate-based	Based on cryptographic digital certificates and avoids passwords in clear text. Can be more transparent for users.	Requires use of in-house or outsourced certification authority. Administrative impact of issuing and revoking certificates is itself a disadvantage.
Token-based	Provides strong, two-factor authentication. Usually, employs one-time passwords that protect against password interception.	Token management, needed by both, users and organization. Cost of tokens.

No.	Particulars	1	2	3	4
4.	Are FTP services carefully implemented? Avoid running an FTP service, that allows users to upload files on the same host, as the web server, as this can result in, arbitrary material being transferred to the host.				

(Contd)

No.	Particulars	1	2	3	4
	If an FTP service is a necessity, consider the following approaches to protect the integrity of the web server: • Use the access control capabilities of the web server, to place strict limits on the directories and files, that can be accessed via, FTP • Use strong authentication for FTP, PUT operations, such as, SSL-based digital certificates • Allow PUT access, only through a separate server instance, run under a separate user ID, that cannot be read by 'nobody' (The user ID for normal access, should not have 'write access' to the document files.).				
5.	Logging Is logging of access, to web pages, enabled and are the logs reviewed?				
6.	User account (a) Is the web server, configured to be a stand-alone unit, without any membership, to any domain inside the bank's IT architecture? (The system should not be added to any domain in the bank. It should be a completely stand-alone system.) (b) Check whether or not, the super user account in the web server, is enabled for login, only on the system console and not from across the network. (This is applicable to all user accounts in the web server.) (c) Check if appropriate parameters are implemented, in the operating system of the web server, so that the super user account will lock out, if too many unsuccessful attempts are made, across the network, but will remain unlocked, at the system console. (This can be implemented at operating system level.) (d) Check and ensure that there is no account, that has privileges, equivalent to those of the super user. (Disable/remove all the default accounts that come bundled, along with the operating system. Remove all the privileges, of all the accounts, except the administrator account.) (e) Better still, check and ensure that there are no other user accounts or system accounts, that are not required to be present in the server, in the first instance.				

(Contd)

No.	Particulars	1	2	3	4
7.	Miscellaneous (a) Check, if sensitive operating system-related, executable program files and data files, on the web server, are stored in a public area, or, in any other secure location, with audit duly-enabled. (b) IP routing should be disabled in the web server. Check and confirm this. (This is required to ensure that no IP packet gets routed, by making this as the firebase.) (c) Ensure that unauthorized ports, e.g., UDP port No. 443, are not allowed inside the web server. Also, ensure that unnecessary services like, ftp, messenger, SMTP, telnet, etc., are not installed and activated on the web server. (d) The facility to shutdown the machine, should be restricted to the system console, on the web server. Check and ensure this. (e) Access to floppy drive, CD-ROM drive, etc., should be restricted in the web server, to an interactive level only, to prevent these devices from being shared by all processes, on the system. Check and ensure this.				

WEB HOST

Although a number of platforms exist, for a web server, for many organizations, the choice will be influenced by:

- The type of web service required
- The availability of in-house resources
- Organizational preference for the brand

Web server software— audit checklist score

1 = Poor, 2 = Not clear, 3 = Needs Improvement, 4 = Satisfactory

No.	Particulars	1	2	3	4
1.	Has hardware been carefully sized? (a) Carry out a careful capacity planning exercise, to ensure that the CPU, memory and disk resources of the host system, are sufficient for the usage expected.				

(Contd)

No.	Particulars	1	2	3	4
	(b) Monitor actual usage of the resources, over time. This will allow upgrades to be applied, in advance of any serious degradation in performance.				
2.	Is resilience built-in? Use well-tested and reliable hardware platforms, with in-built redundancies, geared towards, the levels of availability required. For example: web hosts can be provided with redundancy in: • Power supplies • CPUs • Disk drives • Entire systems: in hot-standby mode, at an alternative location.				
3.	Is physical security adequate? Locate web servers, in a managed and secure, physical environment, to protect them from threats such as, fire, accidental damage and vandalism.				
4.	Configure the operating system carefully (Harden it!) (a) Have all user accounts, except for the web server account(s), web master accounts and authorized administrator account, been removed? (b) Are different root directories, for the web server and server documents, used? (c) Locate interpreters, shells and configuration files, outside the web server directory. (d) Use a dedicated host for the web server and aim to disable all other services, including SMTP and FTP. (e) Ensure that only a minimum set of client applications, is installed. (f) If a browser must be installed, then downloading of active content, for example, ActiveX and Java, should be disabled. (g) Where appropriate, run multiple server instances, under different IDs, to provide different types of access, to different users. (h) Install packet filters, such as TCP wrappers, to restrict connections from known hosts or services, and to log incoming service requests. (i) Are all sensitive files, protected from access through the web, e.g. /etc/passwd, data files, etc.?				

(Contd)

No.	Particulars	1	2	3	4
5.	UNIX (a) Is 'chroot' used on the web server root, to prevent the web server from seeing any part of the normal file system? (b) Is the web server, started as a root user (to open standard ports: 80/443), and then changed to another user ID, for example, www, with minimum privilege? (c) Remove default accounts, for example, lpd and sync, and minimize the number of privileged accounts. (d) Remove compilers, setuid/setgid scripts, and windowing software. (e) Do not run routed (so that, the host's router tables are not, automatically updated). Set the default route to be, the access router. (f) Disable all the services that are not, explicitly required, including NFS, NIS, other RPC-based services, the portmapper, booting services, the 'r' command services, UUCP, and printing. (g) Disable unnecessary kernel services, in particular, the IP forwarding (routing) option, and any service that enables sniffing, for example, tcpdump. (h) See UNIX audit guide, for further information on controlling UNIX systems.				
6.	Windows (a) Use only the NT File System (NTFS). (b) Disable, if possible, both, the server and the workstation, on the host platform. (c) Do not designate the server, to be a domain controller. This will prevent an attacker, who compromises the security of the web server, from gaining domain level access. (d) Do not allow the web server to run as SYSTEM. (e) Rename the administrator account with an obscure name, so that an attacker, would have to first guess the account name. (f) Disable the guest account and all user accounts. (g) Disable all unnecessary network services and protocols. (h) Remove any bindings to NetBIOS, over TCP/IP.				

(Contd)

No.	Particulars	1	2	3	4
7.	Are robust server administrative practices implemented? (a) Restrict, wherever possible, the administrator account, to log in via, the console, only. If this is not possible, the remote administrator login, should be subjected to strong authentication procedures, for example, one-time password or challenge/response. (b) Log the failures and successes of administration operations, log-ins, security configuration changes, and server initializations and shutdown. (c) Consider using tools such as, SSH, to encrypt administration sessions, to prevent information such as, administration passwords from being disclosed.				

NETWORK ENVIRONMENT

The web server, clearly needs connectivity with the Internet and often, also requires access to or from the intranet. The way these connections are established, does not influence only the security of the web server and web application, but also that of the organization's entire IT infrastructure. The network environment of web servers, therefore, needs to be designed and managed carefully. Some of the main issues to be addressed, are identified in the following checklist.

Table 7.3 Where to place the web server

	Advantages	Disadvantages
On external network	• Least risk to security of internal networks • Greatest web server performance • Low manpower costs, particularly suitable for small organizations	• Least control/flexibility • Poor opportunities, for integration with other corporate systems • Only supports a basic web service
Outside firewall	• Low risk to security of internal networks • Increased control and flexibility	• No protection of web server, by firewall • Increased manpower costs, • Increased hardware/communications, costs

(Contd)

	Advantages	Disadvantages
Inside firewall	• Good protection of web server, by firewall • Good opportunities for integration with other corporate systems • Good control and flexibility	• Increased design complexity • Increased hardware/communications • Costs
On internal network	• Web server, protected by firewall • Greatest control and flexibility • Suitable for intranet server	• Greatest risk to internal network • Possible threat from internal users

Network Environment– audit checklist score

1 = Poor, 2 = Not clear, 3 = Needs Improvement, 4 = Satisfactory

No.	Particulars	1	2	3	4
1.	Have bandwidth requirements been estimated? Carry out a careful bandwidth estimation exercise and monitor utilization, frequently. <i>NB:</i> This is one of the most critical factors in preventing overload.				
2.	Is resilience inbuilt? For systems with particularly high availability requirements, consider maintaining a separate Internet connection, through a different Internet Service Provider.				
3.	Have network services been restricted? (a) Limit the services, allowed between the web server and the inner network, to those that are justified by a specific requirement. (b) Do not permit the server, to initiate network connections, but only, to receive and respond to connection requests. (c) Permit port 80 (and/or port 443 for SSL) connection from outside, with ACK bit NOT set, and deny all others. (d) Permit port >1023 connection to outside, in response to the above, with ACK bit set, and deny all others.				

(Contd)

No.	Particulars	1	2	3	4
4.	Have networks been carefully configured? (a) Locate the web server, on a network that does not carry confidential traffic, preferably on a network of its own, a switched Ethernet or an ATM network, to minimize the risk of packet sniffing. (b) Make a careful assessment of the best placement of the web server, in the network architecture. The key points to consider, are outlined in the following points.				
5.	Firewall (a) Ensure that the firewall is correctly placed and that the network is segmented into trust zones. To enforce stricter access controls, on internal and external traffic. (b) Ensure that the firewall ACL is organized systematically. An unorganized firewall rule base, reduces the readability and manageability. (c) Ensure that the implementation process, for firewall rule base addition/deletion, is clearly defined and followed. (d) Ensure that up-to-date documentation of the firewall, including access rights, is maintained and that there is a proper change management procedure for updating it. (e) If the demilitarized zone, where the web server is hoisted, is also connected to the internal network, then it should be ensured that traffic, from the internal network to DMZ, goes through the firewall. (f) Check for the high availability of the firewall. (g) Check for the latest operating system of the firewall (IOS). (h) Check for the ports in the firewall, that should be as per the firewall policy and procedures. If specific computers are allowed special access through the firewall, then auditors should probe further. (i) The only user accounts on the firewall, should be those of the firewall administrator and backup administrator. Only these administrators should have privileges, for updating system executables or other system software. Only the firewall administrator and backup administrator, should be given user accounts on the organization firewall.				

(Contd)

No.	Particulars	1	2	3	4
	Any modification of the firewall system software, should be done by the firewall administrator or backup administrator, and requires approval of the concerned authority.				
6.	Routers (a) The access control list should be configured to: • Drop packets with invalid source address • Allow only those protocols, that are required to pass through (b) Services running on the router: • All unnecessary services running on the router, should be stopped • Use only, corporate standardized SNMP community strings (c) Configuration change and management of router: • Once the initial configuration is done, changes in configuration should be done, only when the working situation demands such a change • Only authorized personnel should be permitted to make changes, to the configurations in the router • All the changes that are made, should be in accordance with the change management policy (d) Administrative control: • Only authorized personnel should have complete control of the router and its accessories like, the TFTP server, • The router should be kept in a physically secure place and should be provided with adequate protection against environmental threats like, fire, etc.				
7.	Intrusion Detection System • Ensure that the bank has a mix of host-based and network IDS, as per the requirements. (a) Important systems, viz. webserver, database server, should have host-based protection, to detect application-specific attacks. (b) IDS logs should be properly monitored and threats, appropriately prevented.				

The checklist mentioned above, is not comprehensive and auditors are therefore advised to customize it, by taking into account, the specific application, web server, web host, firewall, IDS, Router and the relevant, regulatory and Government guidelines.

Box 7.5**Score assessment tips**

1. Scores from 1 to 4 (poor to satisfactory) should be given to all the areas, like, strategy, security management, etc.
2. In case any area (like service level agreement, training, etc.) has not been addressed at all or if the treatment is primitive, the score should be 1. In case the treatment of the area is not clear, the score should be 2. If, in case, the treatment of the area needs improvement, the score should be 3. If the treatment of the area is satisfactory, the score should be 4.
3. The auditor should use his/her discretion in arriving at the score for each area that consists of many sub-areas/sub-points. The relative importance of the sub-areas/sub-points to the overall scenario may be used as a guiding factor in scoring.
4. Calculate the total score from all the checklists given.
5. The minimum score is 46 (46 questions/areas and minimum is 1 per area) and the maximum is 184 (46 questions/area and maximum is 4 per area)
6. Scores from 139 to 184 can be considered “good”, in the sense that both, the management and technical architecture of the bank, are fairly stable and secure and are as per the industry standards.
7. Scores from 93 to 138 can be considered “average”, which means that the Internet banking structure needs improvement. There are both, administrative and technical gaps that needs to be filled up.
8. Scores from 46 to 92 should be considered “poor” meaning thereby, that the Internet banking structure is not secured and should not be made available online, unless the gaps are filled.

SUMMARY

In this chapter, we first discussed the waves in Internet banking, as a sequel to the dotcom hype in 1996, and how the second wave of Internet banking, as a multiple delivery channel, for financial products, has come to stay in the financial market. Web technology, which is the precursor to Internet banking,

was also discussed along with the differences between static and dynamic websites and also, various issues related to web technology.

Then, we discussed the types of Internet banking, i.e. static, semi-transactional, transactional, and pure play. The generic architecture for setting up the Internet banking infrastructure, was also discussed, as were the various options for setting up the Internet banking architecture, in both, centralized and distributed environments. The risks and controls in various architectures were also deliberated on, at length. Then we discussed the multi-layered security approach, wherein we concluded that point solutions, cannot make an Internet banking architecture, secure. You need to have a holistic approach, where each layer, starting from the web browser to the management, should have some control. The risks and controls of all these layers, were also discussed in detail. We then went on to talk about the basics of penetration testing, which is very important, particularly from an Internet banking audit perspective. In the end, we offered a checklist, which is expected to help the auditor, adopt a structured strategy for auditing.

REVIEW QUESTIONS

1. What is web technology? How does it work? Describe in brief.
2. What is the difference between, static and dynamic web content? Describe the risks involved, in both.
3. Describe the various issues involved, in web technology, from an Internet banking perspective.
4. Who is an Internet Service Provider (ISP)? Describe the hierarchy of ISPs.
5. Describe the security implications of choosing a particular ISP.
6. Describe the generic architecture of Internet banking and discuss its components.
7. What are the various options of Internet banking architecture, in a distributed environment?
8. Discuss the various options of Internet banking architecture, in a centralized environment.
9. What is multi-layered security approach, in Internet banking? Discuss in detail.
10. Write the various steps, required to conduct an Internet banking audit.
11. Discuss the basics of penetration testing.

MULTIPLE CHOICE QUESTIONS

1. Pure play internet banks are:
 - (a) Banks with no brick and mortar structure, but which provide Internet banking services
 - (b) Banks with no brick and mortar structure, but which has an arrangement with other banks, for providing Internet banking services
 - (c) Banks which provide Internet banking demo, through the Internet
 - (d) Banks which provide static Internet banking services, to the customers
2. Which of the following statements, regarding CGI script and pure HTML, is not true:
 - (a) Both are interpreted languages/scripting
 - (b) Both are server-side scripting/language
 - (c) CGI takes input from HTML, and gives output in HTML
 - (d) Both the codes are physically sent to the client's browser, through the HTTP protocol
3. Which of the following is the most correct, about the World Wide Web (WWW)?
 - (a) The World Wide Web (WWW), is a network of web servers, which provides a mechanism to link pages
 - (b) WWW, is a collection of web servers in any enterprise
 - (c) WWW, is a network of web servers over the Internet
 - (d) WWW, is a collection/network of web server over intranet
4. In a client/server architecture, a Domain Name Service (DNS) is the MOST important, because it provides the:
 - (a) Address of the domain server
 - (b) Resolution service for the name/address
 - (c) Resolution on the Internet for the name/address
 - (d) Domain name system
5. Which among the following, is not true Internet Service Providers (ISPs) are:
 - (a) The companies that own and provide access to the Internet
 - (b) The companies that provide links to the Internet backbone
 - (c) The companies that provide collocation of mail servers

- (d) The companies that provide the Internet link and a set of IP public addresses
- 6. Which of the following is true of Digital Subscriber Loop (DSL)?
 - (a) It is a broad band connection
 - (b) It is phone line, to be used for both, normal telephone lines and also, full time interface
 - (c) It is an asymmetric connection
 - (d) All of the above
- 7. The most important requirement, for running automated tools, for vulnerability scanning are:
 - (a) The tool should be authentic
 - (b) The tools should be run by professionals, otherwise they will spoil the system
 - (c) The tool should be from a reputed company
 - (d) The tool should take into account, the latest threats and vulnerabilities
- 8. Penetration testing of network, involves:
 - (a) Scanning the ports of the operating systems
 - (b) Scanning the ports of all the systems
 - (c) Scanning the ports of the devices, at the gateway
 - (d) Scanning the ports of the firewall and routers
- 9. The delegation of authority and authorization, in WWW technology, can be best addressed by:
 - (a) Taking care of this, at the operating system level
 - (b) Taking care of this, at the DBMS level
 - (c) Both A and B
 - (d) Developing a specific security code, by the web application developers, to provide a finer, granular access to corporate resources
- 10. Which among the following, is the most appropriate regarding penetration testing?
 - (a) Penetration testing is conducted by using automated tools
 - (b) Penetration testing will help the organization in rectifying vulnerabilities
 - (c) Penetration testing is conducted to detect the known vulnerabilities
 - (d) Penetration testing cannot be done, without using any tools

DISCUSSIONS AND RESEARCH QUESTIONS

1. Internet banking audit, is a hybrid of both, application control and network control review. Discuss.
2. “The second wave of the Internet as a multiple delivery channel, has become pervasive and has come to stay, in the Indian banking and financial market.” Discuss.
3. “Putting your house in order is the best solution.” Discuss in the context of security implications of choosing a particular ISP.
4. Describe the philosophy behind the multi-layered security approach, for Internet banking and discuss the risks and controls related to the various components.
5. Discuss critically, the auditing aspects of the management practices, of Internet banking.

EXERCISES

1. Draw a security architecture of Internet banking, in a centralized environment and a four-tier application model, with appropriate redundancy, in each component, wherever necessary.
2. Draw an Internet banking secured architecture, for a bank that wants to deliver Internet banking, both, from their centralized database, and some distributed database.
3. List the risks and controls of the browser layer, of Internet banking.
4. Go to the internet site of the Reserve Bank of India at www.rbi.org.in and summarize the Internet banking report available. (You can take the help of your faculty/ demonstrator, to find this document on the site.)
5. Prepare a checklist, for auditing the web server, in an Internet banking scenario.

8

Operating System—Risks and Control

-
- ❖ Types of operating systems
 - ❖ System configuration
 - ❖ Operating system capability
 - ❖ Functional components of operating system
 - ❖ Operating system services
 - ❖ Access control
 - ❖ Utility software—the weak link
 - ❖ Hardening of OS
 - ❖ OS security
 - ❖ Control in operating system
 - ❖ OS control checklist
 - ❖ Security checklist for Linux
 - ❖ Security checklist for Windows 2000
-

OPERATING SYSTEM (OS)

An operating system is a program that acts as an intermediary between the user of a computer and the computer hardware. It allows for the execution of user programs and makes solving of user problems, easier. It also controls the execution of other computer programs and provides different services to the user. The operating system is a critical part of any IS and since it is the interface between users, application programs, and the resources deployed in an IS, breaches in the integrity and reliability of operating system controls, could lead to serious losses for an organization.

To understand operating systems and associated controls better, it is important to understand the various system configurations that are typically

seen in an IS and how the OS plays a role in each one of these environments. The risk quotient of the breach in OS control, in each configuration, is different and it is crucial for an auditor to understand different environments and how an OS is used in these environments to ensure adequate risk assessment and control deployment.

TYPES OF OPERATING SYSTEMS

Over the past many years of evolution of computers, we have witnessed a remarkable growth and change in the capabilities of an operating system. The capabilities of the operating systems varied, based on the different system configurations that were used by users.

To understand the capabilities of different operating systems, we will first look at the different system configurations and then at the related, specific operating system capabilities of these configurations.

SYSTEM CONFIGURATIONS

Over the past few years, PCs have become synonymous with computers, but these actually form only a very small percentage of computers in this world. Computers come in different sizes and configurations and have a specific purpose to serve. We will now discuss, some common system configurations and their purposes, to set a framework for identifying risks and control requirements for the OS, used in these environments.

Mainframe System

This is a large computer system, serving hundreds of users and providing complex business-oriented services for the users.

Over the past few years, mainframes have become crucial components for the business systems of many companies. They have been used for a long time and have a lot of legacy applications, serving business needs. With the advent of web-based solution delivery and technologies, it is now imperative that many of these legacy applications be web-enabled. Usage of mainframe systems, now concentrates on migrating legacy applications into a web infrastructure.

Some of the core strengths of mainframe systems include, scalability of high-volume transactions and high-server performance.

Desktop Systems

These are the systems that have increased the popularity of computers greatly and ensured the extensive usage of computers in homes and in organizations. These systems, provide many features to the users, to enable ease of use and also have a very large number of business and personal applications that are built for this category of computers.

The presence of these computers in personal and business environments, entail great risks and threats to the IS, deployed in the organization. The ease of use of these systems, allows users to use them in varied ways and this could leave several loopholes in the security structure, within the organization.

Distributed Systems

With the penetration of powerful desktop systems and extensive usage of networks in IS environments, distribution of processing power, among multiple servers, has become popular especially in the case of high processing, intensive systems. For these kind of systems, the OS requirements are different and must provide specific features that allow applications to provide distributed services to the users. These operating systems, allow resources to be identified, shared, and accessed in the distributed environment, transparently, so that the users do not really need to know where the resources are deployed in the system.

These kinds of systems, face special kinds of risks, the occurrence of which can be minimized by putting in place, relevant OS controls.

Real-time (RT) Systems

Apart from the business and personal systems, that have been discussed, computers are used for real-time systems like manufacturing, etc. For real-time systems, the OS is specially built, based on the RT environment and provides a limited set of features that are required only for these environments.

Embedded Systems

With the miniaturization of processors and other components, computers have found a place in a wide range of devices that have computers embedded in them. We find computers in systems like watches, cell phones, security devices, and many others.

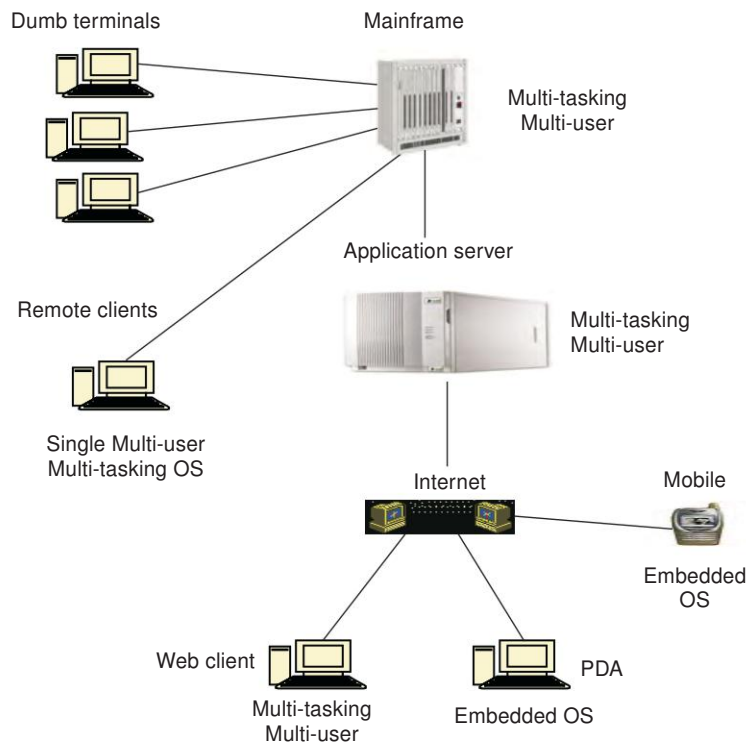


Fig. 8.1 A sample Information System

OS CAPABILITIES

Multi-processing/Tasking Operating Systems

Operating systems allow users to execute tasks/ jobs on the system. Each task/ job is referred to, in OS parlance, as a process. The ability of an OS to make the user believe that multiple jobs are being performed by the system, simultaneously, is called multi-processing.

Most computers do not have parallel processing capabilities, but owing to the speed of the computer and the inherent delay in perceptions of users, the OS can shift control, between different processes, at a very high speed, to give the users the feeling that multiple processes are being executed simultaneously, whereas actually, only one process is executed in the system, at any given point in time.

Some of the OSs that have this capability include, different flavors of UNIX, Linux, Windows NT, Windows 2000, Windows 98, etc. This feature has become a core feature of most operating systems.

Some of the earlier OSs like MS DOS, etc. were single-tasking operating systems which did not have the ability to execute multiple processes, at the same time.

Multi-user Operating Systems

OSs, which had the capabilities of multi-tasking, allowed multiple tasks to be executed, at the same time. Hence, as an extension of the concept (multi-tasking), allows multiple-users of the system to perform tasks on the system, all at the same time. The OS which allows multiple users to use the system, at the same time, is referred to as a multi-user operating system.

Most recent operating systems are capable of providing multi-user support. Some examples of multi-user operating systems include, UNIX, Linux, Windows NT, Windows 2000, etc.

Multi-user operating systems, are characterized by the ability to host multiple users, but with this strength, comes greater threat and responsibility. The administrator of the system should ensure that users and resources on the system are protected from other users and also against intentional or unintentional misuse/exploitation.

Embedded Operating Systems

With the miniaturization of chips and processing components, computers have become a part of most daily-use devices and systems like watches, network components, controllers, mobile phones, PDAs, etc. To support the applications in these devices, special capabilities are required. The OS for embedded systems, are unique, in terms of resource utilization and other aspects because typically, they have to work with very limited resources.

FUNCTIONAL COMPONENTS OF OPERATING SYSTEM

Process Management

All operating systems allow application programs to be executed in a specific context, to provide services to the users. Each application, running on a computer is called a process and one of the major functions of an OS is to manage these processes and allocate resources to them. Since the processes,

access and use resources, on behalf of the users, the OS needs to control the processes, to ensure that they do not misuse the available, resources.

Some initial desktop operating systems like MS DOS, CP/M, etc. were single-processing operating systems, which allowed users to execute only one process, at a time.

More evolved OSs like UNIX and Linux support multi-processing, using techniques like, timesharing where the OS shares a given time slot for each process.

The tasks of allocating priorities and time slots, and starting, suspending, and stopping the processes, is the job of the process management component of the OS. Different OSs use different process-scheduling mechanisms, like *Round Robin*, *Most Recently Used*, etc. to decide on which process should be scheduled for the next time slot. Most of the recent operating systems, also possess the ability to assign and dynamically change priorities of the processes, to use resources more efficiently.

Process management is usually performed in the following ways:

- Cooperative process management
- Preemptive process management

Cooperative Process Management

Some operating systems (with simple process management capabilities), depend on the processes to relinquish control, over the system and hand them back to the OS, so that the OS can schedule another process, to use the system resources. This is a simplistic mechanism of process management and was used in operating systems like MS DOS.

This kind of a system has inherent problems with rogue processes that do not relinquish control, over the system resources. In such an event (if the process hangs), the OS will not be able to pass on the control to an other process and will hang. A typical example of this kind of process management is MS DOS, where if one of the processes hangs, the whole OS hangs.

Preemptive Process Management

The inherent weaknesses of cooperative process management, make it evident that most serious operating systems, cannot depend on this kind of process management.

To overcome the weaknesses of cooperative process management, most operating systems use another method called preemptive process management where, the OS has greater control over activities like process initialization,

suspension, and termination. The OS allocates resources, for a specific duration to the processes and preempts the processes if the duration is exceeded. This ensures that if any of the processes hangs, the OS can still suspend the application and allow the other processes to function properly. Most of these OSs also come with capabilities to terminate the rogue processes on user request.

Some of the most common OSs which use preemptive process management, allow dynamic process priority management. This feature allows the users to instruct the OS to increase or reduce the priority of processes at run time.

Main Memory Management

All processes, use memory for temporarily storing data and instructions. When the processes are executed in the memory, it is vital that the memory, used by a process, to store information, is secured and that one process cannot access or delete information, owned by another process.

Also, the OS, typically controls the use of memory by different processes, to ensure that no process can capture all the memory and thereby cannot cause the Denial of Services (DoS) for other processes.

File Management

The file system is an integral part of any operating system, with a direct user interaction. The programs, data files, and other information in any computer are stored persistently (for a long duration), in an easy-to-use and manage file system on secondary storage.

A file is a contiguous, logical address space, storing data which is numeric, character, or binary. Depending on the type of the data, the OS allows access to the file in different ways, and associates these files with various applications that can access the files.

File Properties

Most OSs identify the following parameters for files: name, type, location, size, access privileges, time and date of creation, modification and access. All these parameters are controlled by the file system manager. The features that are provided by the file system (FS) component of the OS define the ease of use, stability, and robustness of the OS.

File Actions

The file system component of the OS, provides the following actions to be performed on the files. These actions form a basis for defining of a protection access matrix that ensures secure access to files in the system.

The file system allows:

- Creating files
- Writing files
- Reading files
- Deleting files
- Repositioning of file pointer, within the file, i.e. file seek
- Opening files
- Closing files

File Types

The file type of a file is an important attribute that defines how the OS and other applications should treat the file. Based on the type of the file, the OS gets cues about which application is associated with the file's operations, thus, making it easy for users to access files and view their content. In most systems, the type of the file is explicitly displayed, as part of the file name, as an extension that gives the users a visual clue about the content in the file.

The file types are typically associated with the OS level through, what are called mime types. These types are industry standard lists of file types. The OS uses a map to associate the file, based on the type, with an application that is used, to perform operations on the file.

Some common file types are listed in Table 8.1.

Table 8.1 OS file types

<i>File type</i>	<i>Usual extension</i>	<i>Functions</i>
1. Executable	exe, com, bin or none	Read to run machine language program.
2. Object	obj, o	Compiled, machine language not linked.
3. Source code	c, cc, java, pas, asm, a	Source code in various languages.

(Contd)

<i>File type</i>	<i>Usual extension</i>	<i>Functions</i>
4. Batch	bat, sh	Command to the command interpreter.
5. Text	txt, doc	Textual data, documents.
6. Word processor	wp, tex, rrf, doc	Various word processor format.
7. Library	lib, a, so, dll, mpeg, mov, rm	Libraries of routines for programmers.
8. Print or view	arc, zip, tar	ASCII or binary file in a format for printing or viewing.
9. Archive	arc, zip, tar	Related files, grouped into one file, sometimes compressed, for archiving or storage.
10. Multimedia	mpeg, mov, rm	Binary file containing audio or A/V information.

Directory Structures

After a lot of development and research on advantages and disadvantages of different file system organizations, it was found that directory storage, that is common to most operating systems, is a very flexible, extensible, and easy-to-use way, for the organization of files, in a file system.

A directory is 'a special file that contains references to various other files that are said to be contained in this directory'.

A very crucial aspect of the OS is to ensure that files in the secondary storage are secure, so that unauthorized access and modification of the resources, cannot be done by the users. It is the file management component of the OS that ensures that users can store files securely, with adequate access control privileges. Any breach in the security of files could lead to catastrophic conditions, because any process that executes, is stored in the file systems, as is the data used by the applications.

Any compromise to the integrity of the file system, could lead to severe security breaches.

So controls over the file system, form a crucial part of any OS control framework.

Input/Output (I/O) System Management

Since the OS is the interface between devices and the users, all I/O operations performed on the devices, connected to the system, are controlled through the I/O management component of the OS.

This component, controls various devices like, keyboards, monitors, floppy disks, hard disks, USB ports, network interfaces, and many other input and output devices.

The following diagram shows the connectivity of I/O devices to a computer. The way these devices are referred to and accessed, is controlled by the OS.

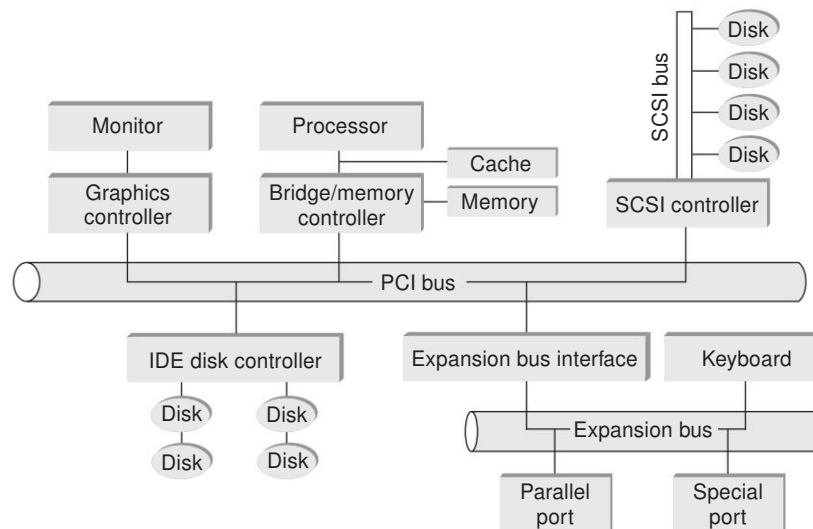


Fig. 8.2 Source: Operating system concepts, Silberschatz and Galvin

Most I/O devices are connected to something called a 'Bus' that is a common gateway for the data to flow to and fro, between the various devices and the computer. Depending on how the OS I/O subsystem works, these devices are accessible to the users as resources, through the file system.

It is the job of the I/O subsystem of the OS, to ensure that when access to a device is provided to a user, through the file system, the I/O device provides the services to the user. Usually, when devices are installed, various device drivers are also installed, to ensure that they can interface with the OS properly, and the OS can allow access to these devices to the users.

With great advances in the secondary and tertiary storage devices, security remains a critical concern. This entails a serious need to analyse how the I/O system access is controlled from the file system and which I/O devices should be enabled or disabled for secure use of the system.

For example: Enabling access to USB ports for critical servers, could be a security risk, as users have the ability to plug-in USB memory sticks and copy confidential information to these.

Network Management

The prevalence of networking and popularity of the Internet/Intranet in organizations, has made networking a crucial component of the OS. It is difficult to imagine a system, without some kind of networking component. This is the reason for the now, common pattern in all operating systems, to include the networking subsystem as an inherent part of the OS.

Some years ago, separate network operating systems were developed, since the OS itself, did not have networking capabilities. But these days, it is rare to find an OS, without inbuilt networking capabilities.

The networking component of an OS, performs the functions of identifying, accessing, and managing resources over the network and allowing controls to operate over the network resources.

Many early OSs like, DOS, etc. did not have an inbuilt networking component in the OS. So these OSs, could not support networked operations and were used for only single-user desktop usage.

Over a period of time, with network infrastructure becoming more prevalent, the support for networking was provided by separate network operating systems. Some popular examples of network operating systems that were used to support non-network capable OSs include, Novell Netware, Banyan Vines, etc. These OSs, provided the networking capabilities with which, computers could be networked.

With the growing popularity of networking and increasing maturity of the desktop OSs, networking capability has become part of most, present day operating systems like, Windows 2K, Windows NT, and later versions of Windows.

Operating systems like UNIX and Linux had, from their early versions, provided capabilities for network connectivity and TCP/IP support.

Protection System

Any OS consists of a collection of objects (resources), i.e. both, hardware and software. Each resource is assigned a unique name and can be accessed through a set of operations, allowed for different users.

The problem of protection involves, ensuring that access to every resource in the system is controlled and only those resources and users, who are allowed to access particular resources, are allowed to do so. Protecting resources also involves, ensuring that the users who are allowed access to resources, can perform a predefined set of tasks on the controlled resources.

A typical protection implementation is associated with the following two concepts:

Access rights: an associated set of resources and rights that are allowed on this resource.

Domain: a set of access rights that are allowed in the system, also referred to as roles in the OS. Depending on the role of the user, access controls are defined. This set of access rights is called a domain. For example, in UNIX there are two default domains, viz. *Normal user*, *Super user (root)*. Depending on the role of the user, the access rights are controlled. In Windows, apart from the *user* and *administrator*, another domain called *power users* also exists.

Implementing protection/security in a system involves, defining multiple domains of users and the access rights that are allowed for users in these domains, on various resources.

OPERATING SYSTEM SERVICES

This section describes some of the functions of an OS and provides a comparison to show how different operating systems, provide these services. Figure 8.3 describes the mechanisms through which a user interacts with the hardware and the services that the OS provides to the user.

Program Execution

Running or executing programs, is a core function of an OS. These services are offered by the process management component of the OS. After the OS is loaded (booted) into the system, users can use the system through applications. Matured OS provides capabilities to the user for starting processes, changing priorities of the processes, stopping processes, etc.

The complexity and maturity of the OS are defined by the capabilities that the process management component possesses. Some of the capabilities of the OS, in terms of program-execution include:

1. Application startup
2. Memory allocation for the process
3. Ability to execute a program in the background or foreground
4. Ability to schedule processes at specific times, in the future
5. Ability to allocate permission to the process, based on user privileges
6. Ability to modify permissions of the process, at run time
7. Ability to monitor process resource consumption
8. Controlling resource consumption on a per process basis
9. Ability to suspend processes for a temporary period, to be started again
10. Ability to schedule processes and context switch, between processes, in a multi-tasking environment
11. Ability to change the priorities of processes
12. Control over process termination
12. Controlling rogue processes

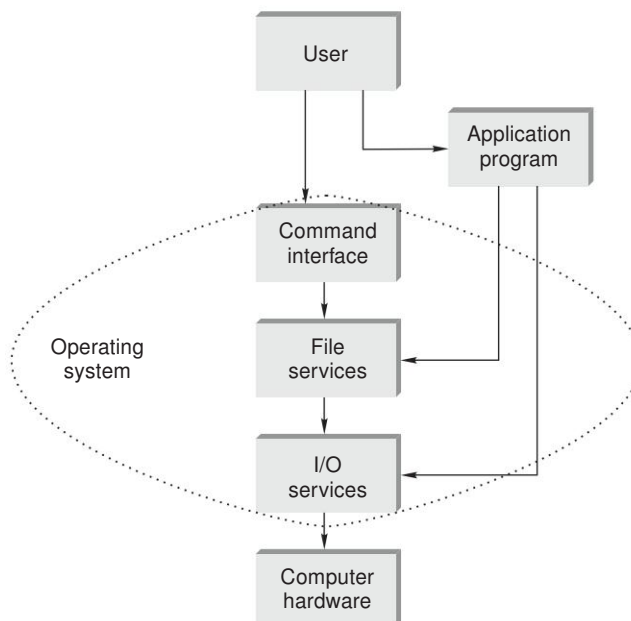


Fig. 8.3 Operating system services

Resource Allocation

The ability of an OS to allocate various resources like memory, Interrupt Requests (IRQs), Direct Memory Access (DMAs), etc. for processes during their execution and to control access to these resources, based on the security privileges of the users/processes.

File System Manipulation

The ability of the OS to create, store, and retrieve files and data from a file system, defines how users can store information/ data, applications/programs in a system. The ease with which the OS allows the users to find, access, modify, and control files in the file system, defines the core behavior of the OS.

Files are the most frequently used resources, by users in an OS, because all devices, resources, and entities in an OS are manifested to the users, as files, for consistent access to all these resources.

Goals of File System Organization

The file system component of the OS has a very important task of organizing data on physical storage and provide access to users to various devices that are typically provided through a file system entry.

The goals of the file system are to ensure:

- Easy-to-use organization of files
- Easy and effective access mechanism that can grow
- Ability to host different devices and provide access to them
- Ability to effectively control access to resources by users

Some of the not-so-common functions, include:

- Hosting file systems from remote locations (sharing remote directories)
- Linking one location of the FS to another

Over the past many years, file systems have evolved steadily and are mature solutions that make access very easy, for users.

Depending on the GUI features, provided by the OS, the file systems also provide a relevant UI for users, to access the file system.

File Sharing (FS)

As mentioned above, one of the important goals for a FS is to help access files and resources, provided by the OS and the system, through a standard file interface.

Initially, most FSs, in single-user OSs, were content with allowing the users, access to resources on the same system, but with the growth of networking technologies and the ability to have a network of computers with distributed resources, it became crucial to be able to access remote resources (resources hosted on different machines), with relevant access control privileges.

The current file systems, provide many advanced features for remote resource access and sharing of resources for remote access.

Some of the FS technologies that provide these features include:

- **Network File System (NFS):** A very evolved and standard network, resource-sharing service that is popular on UNIX. This system allows users to share file systems on different machines and access these file systems from remote machines. This is the most common sharing mechanism, operative between UNIX and Linux servers.
- **NetBIOS (Network Basic Input Output System):** Is a Windows-specific protocol that is used to identify and share resources on pure, Windows networks. This protocol, allows users to be able to access files by just accessing a machine as `//MACHINE_NAME/share-name` and mapping this resource onto the local file system.
- **SAMBA:** Is a cross platform file sharing service on UNIX and Linux platforms. This file system, allows users to share resources on Linux or Windows and network platforms and access them from other OSs.

This is a very important service, especially in organizations that have Muti-OS environments, where resources are hosted and shared from Linux, UNIX, and Windows machines.

SAMBA provides inter-operability and resource-sharing between Windows and Linux, by implementing the NetBIOS mapping protocol. This allows Linux to be able to provide SAMBA shares, as NetBIOS shares, to users on Linux machines, to access them. This service also allows the users on Linux to access the Windows shares, on their local Linux machines.

File System Protection

The file system component, performs some of the most important functions in terms of allowing access to system resources, through the file system. The protection of resources, according to user requirements, is the most important job of the file system. Robust, mature operating systems, provide users with advanced mechanisms to protect the file system.

The protection mechanism of the file system is not generic and depends on the OS that is being used. A single-user OS typically, has much lesser FS protection systems, as there is only one user who is expected to use the system. These OSs like, MS DOS, Windows 3.11, etc. have very rudimentary file system protection schemes.

OSs like, Windows 95, Windows 98, Windows NT, etc. have evolved and the file systems in these OSs have matured, over a period of time. But due to evolution from a single-user environment and being driven by backward compatibility issues, the file system's protection mechanisms for these OSs is still weak. However, recent Windows operating systems like, Windows 2000 and Windows XP, provide greater file system protection mechanisms that are based on per user, configurable, access control rules.

Operating systems like, UNIX and Linux have been prominently built to use different pluggable file systems and the security of these file systems is based on individual file system implementations.

But, irrespective of the file systems, the protection paradigm has been consistent and is based on the OS security mechanism. File protection also follows the domain model, where resources (files and directories) in the file system are provided access, based on the domain that the user/application belongs to.

For example: In Windows, the common file system access control matrix includes, SYSTEM, Administrator, Power User, and User domains and the access controls for various resources in the file system are controlled, based on these domains.

With later versions of the Windows OS, security of the FS has improved and files/resources are now specifically marked, with details of ownership and access is controlled, under the domain model.

In UNIX, the file system protection mechanism is driven by well-know (user, group, other) privileges, i.e. all resources in the file system are assigned user-specific group-specific and other privileges.

The protection level of a resource in UNIX, is defined by three octal numbers and the ownership of the resource.

For example: The file `/etc/passwd` is owned by `root` and belongs to the group `root`, and has privileges defined as `-rw- rw- r--`, where the owner of the file can read and write to the file, the users belonging to the `root` group can read and write to the file, but others can only read the file.

Commonly-used File Systems

The following table, describes some of the commonly-used file systems and their capabilities, as available in various operating systems.

This table describes what kind of access is provided to a FS from a specific OS.

Table 8.2 File system in an operating system

Read FS: From OS:	FAT	VFAT	(V)FAT32	NTFS	HPFS	EXT2/EXT3
Dos/WIN 3.X (FAT)	Full access.	No long filename support.		Read-only access. No long file name support.	Read-only access. No long file name support.	Read-only access. No long file name support.
WIN 95 (VFAT)	Full access.	Full access.	Full access.	Read-only access.	Read-only access. No long file name support.	Read-only access.
WIN-NT (NTFS)	Full access.	Full access.	Read- only access.	Full access.	Full access.	Read-only access.
OS/2 (HPFS)	Full access.	Full access.	Full access.	Read-only access.	Full access.	Read-only access.
LINUX (EXT2/ EXT3)	Full access.	Full access.	Full access.	Read-only access.	Read-only access.	Full access.

USER INTERFACE (UI)

Another very important function of the OS is to provide a user interface for the applications that the user accesses. The ease of use of the user interface has

been one of the major reasons for the popularity of MS Windows and has led to its domination in the OS market.

The user interfaces that the OS provides to the users, include:

Command Line Interface

The command line interface has been the most commonly-used UI in most of the earlier versions of the OSs, especially UNIX. This was a very fast and effective way of using the system, especially for experienced users and developers. With UNIX being used in the educational and military domains, this became a very popular interface that users were provided with.

Graphical User Interface (GUI)

During the early 80s, work on providing a graphical user interface was in progress and there were also efforts to build an X-Windows-based system, where users could access the server through what were called, XTerms (X-Terminals). These were among the earlier GUI versions that were used, instead of the command line interfaces that existed at that time.

The acceptance of this GUI on UNIX has been slow and took its time. But based on this concept of Windows, Microsoft released its first version of the now, universally popular MS-Windows suite of operating systems, which made it very easy for users to use the system. Today, it has become a hit with users of PCs and business novices.

The capability of the OS, to provide a standard and consistent UI is very crucial for the acceptance of the OS and enhances the usability of the OS. It is the role of the OS to provide a consistent UI experience, for using any application on the OS.

Operating Systems like UNIX, and Linux, do not contain the GUI (windowing) layer, integrated into the OS, but allow the user to choose different GUI experiences, depending on the user's convenience.

Other operating systems like, Windows, integrate the GUI with the OS, to provide a consistent user experience, which makes it very easy for users to get used to new applications that are deployed, as the look and feel would be similar to what the user is already comfortable with. This is one of the reasons for a satisfying user experience of MS Windows and its popularity.

Network Communication

Before the extensive spread of networking technologies and the Internet, most operating systems did not have networking capabilities as an integral component of the OS. These kinds of OSs include, MS-DOS, Windows 3.11, etc.

But as technology developed and the need for networking grew, the networking component that was external to the OS started being incorporated as an integral part of the OS and this allowed computers to be connected into a network, without any external help/components.

Support for networking implies that the OS has a networking component that implements different layers of the OSI, i.e. inter-networking stack, so that computers can be connected together in either a LAN or WAN.

Before the advent of the TCP/IP, UNIX provided networking capabilities by the support of something called UNIX networking, which was a set of tools, for communicating between various computers in the network. But with the advent and popularity of Internet technologies, TCP/IP has become the default standard for networking on most UNIX/Linux-based networks.

In case of the MS-Windows, the initial OSs did not have any networking capabilities and used third party networking systems like Novell Netware or Banyan Vines, to connect computers in a network.

Later versions of Windows, incorporated the networking suite, integrally, into the OS and allowed users to connect to each other through something known as NetBIOS. It was now, possible to connect Windows networks with other networks, with the support for TCP/IP, available on most Windows OSs, as an optional networking protocol that could be installed.

Program Installation/Upgrades

Easy installation and usage various applications on a system, is usually the primary perception of the users about an OS. An OS that allows installation of applications/programs at the click of a button, would be very attractive to users. Since this would help them go about their business activities, rather than go through the various travails of installation and uninstallation.

This is another reason why, MS Windows is very strong and allows users to install applications at the click of a button, with special setup programs that install the application and perform various installation time jobs, automatically, without or with little user intervention.

The same ease in uninstalling the software, is evident in MS Windows and ensures that users do not have to be burdened with specific technical information about the OS, the environment, or the application itself.

UNIX and Linux, also have similar application installation programs that allow users to install servers, applications, and tools very easily. Different flavors provide different mechanisms, but RPMs are a very popular mechanism for creating installation bundles and using them for installing applications, by the clients.

After installing an application, it is common for users to expect and want multiple updates that are available for installation on the original application. Though the update mechanisms are typically based on the application itself, the OS that provides a simple upgrade mechanism is preferred to something that takes the user through a tedious uninstallation, reinstallation process.

Error Detection

The ability of the OS to ensure correct computing by detecting errors in the CPU and memory hardware, in I/O devices, or in user programs, is referred to as *error detection service*.

The ability of an OS to allow users to identify errors, rectify these and continue working or at least close down the OS, without loss of data, is very crucial for a good user experience.

Effective error-detection and control is very important, since the OS should ensure that an error in one component, does not corrupt the OS or other applications and does not cause loss of data for the user.

For a long time, most Windows OS versions suffered on this front, as they did not have effective error control mechanisms. This caused applications to crash, leading to loss of data and the inability of the user to continue further (popularly called the blue screen error). Also, with earlier versions of the OS, it was very difficult for the user to correctly send a report on the error condition, to the application developer, for speedy correction.

Current operating systems provide a semi-automated/ completely automated mechanism for error-detection and reporting, that ensures that all the information, relevant to the system condition, at the time of the occurrence of the error, is sent to the application developers.

In some cases, the error-detection system also gives the user, relevant help and tutorials to be able to easily rectify an error. If this does not solve the problem for the user, the OS also has provisions for leading the user to the most relevant resources on the Internet, for effective resolution of the problem.

Accounting and Auditing

In any operating system, it is required that resource utilization and user operations of the user, have to be monitored regularly, for better control over the system.

Most operating systems provide some common mechanism for logging each user operation and also resource utilization on the system, during the operation of the system.

These tools can be used for generating an accounting audit trial for selected users, to track the operations performed by the user, on the system. Other tools provide the ability to generate an operational audit trial, so that the user/administrator can identify the level of resource utilization and also track errant/overuse of resources in the system.

ACCESS CONTROLS

Goals of Protection

The goal of the protection service is to ensure that each object is accessed correctly and only by those applications and users that are allowed to do so.

Domain of Protection

As discussed above, the standard mechanism for protection implementation is through the definition of entities called domains that define the rules for access control, over resources.

Access Matrix

Depending on the domains of protection paradigm of security implementation, access control is defined by a matrix that defines the access controls, with columns representing the resources available and the rows identifying the domains defined in the system.

The cells in this matrix, define the access privileges that the domain has on each and every identified resource.

Implementation of Access Matrix

A sample access matrix is shown in Table 8.3.

Table 8.3 Access control matrix

<i>Resource Domain</i>	<i>F1</i>	<i>F2</i>	<i>Laser printer</i>	<i>D1</i>	<i>D2</i>	<i>System registry</i>
System admin	RW	RW	RW	RW	RW	RW
Power user	RW	–	RW	–	–	RW
User	–	–	RW	RW	–	R

The above table, shows a simple access matrix that identifies a set of two protected files, a laser printer, two protected directories, and the system registry (maybe to define installation privileges).

The domain model, identifies three domains (roles/types) of users and allows the system admin category of users to be able to read and write to all the resources.

The power user can access F1, Printer, and the system registry to install applications.

Normal users have access to the printer, D1 and can only read the system registry.

This kind of implementation of the domain model, is a common way to implement of the mandatory access control mechanism that ensures that all the resources that need to be protected, are identified and specific privileges are provided to groups of users, based on the domain they belong to.

UTILITY SOFTWARE

Most operating systems, come with a set of utility software, intended to provide easy-to-use tools for administration, monitoring, and management of the systems.

Most of these tools are provided for the use of the administrators, for specific system administration jobs.

The utility software is used to perform the following:

- Specific security or integrity related tasks. This is done with the help of:
 - Virus scanners
 - Disk recovery tools
 - Unerase tools
 - Software inventory manager/registry manager

- Static security analyzer
- Dynamic security analyzer
- Access control analyzer
- Password crackers, packet sniffers
- Spy software
- Utilities for accessing data quality, which include:
 - File search tools
 - Query facility
 - Memory dump/lister
 - Data comparison utility
 - Access control list validators
 - Backup tools
- To facilitate system understanding, the following are made use of:
 - Configuration analyzer
 - Execution path-mapper
 - Transaction profile analyzer
 - Hierarchy charter
- To facilitate assessing of program quality, the following are made use of:
 - Test data generators
 - Program execution tracers
 - Execution path monitors
 - Network simulators
 - Terminal emulators
 - Online debugging facilities

Utility Software—The Weak Link

Most of the utility softwares listed above, are useful tools, available to administrators and users, to perform regular administrative tasks. These tools are expected to be used with care and to also provide great strength to the user. These tools have capabilities that override the usual OS security preferences and circumvent the usual OS controls.

Hence, it is crucial that the usage of utility software, is tracked and monitored with care.

Some of the common risks, associated with such software include, exploits of spyware that capture passwords and also text, entered during the operation of the system.

Normal usage of the spy software would involve logging the behavior of users and tracking the usage of resources by users. However, an unauthorized installation of this software, will allow users to capture passwords of other users, not only on the existing system. It will also enable the users to access the security and confidential information of other users, including passwords, on different servers and passwords of personal E-Mail servers, etc.

Hence, usage of utility software should be very strictly monitored and should be allowed, only on receiving express permission/authorization.

HARDENING THE OS

What is Hardening

The process of securely configuring a system, to protect it against unauthorized access, while also taking steps to make the system more reliable, is referred to as hardening of the system.

Hardening of the system is done at multiple layers, including the hardware infrastructure, OS, processes, and applications.

This section discusses the concepts and steps involved in hardening the OS, for securing the system.

Rules for Hardening

There is no standard set of rules for hardening a system, but the steps involved in hardening a system depend on various factors including:

- Hardening of hardware-related configuration
- Network-related configuration
- System configuration
- Stand-alone system
- Networked workstation
- Multi-user server
- Application server

Though the specific steps involved in hardening a system differ, based on the above parameters, this section, lists a few common guidelines that are used in hardening systems.

Some of the more commonly required hardening steps include:

- Keeping track of security patches, hot fixes
- Using secure file systems
- Controlling services
- User controls including account and audit policies and procedures
- System security settings and options
- Network settings

A detailed security checklist has been provided, later in the chapter.

OS CONTROLS

From the past few sections, it is evident that the OS plays a very important role in an IS. Also, since it is a portal to the resources that are accessible to the users and programs, controls that are available at the level of applications or networks or other layers, can be compromised, if these resources are not adequately controlled.

The integrity and reliability of the OS, is crucial to ensure that various resources and controls are not compromised.

This section describes the nature/requirements of a reliable operating system, possible threats to the OS integrity and a framework of controls for the operating system, for secure operations.

OS SECURITY

Nature of Reliable Operating System

The goals of an operating system, as identified by Stepczyk (1974), are very pertinent even today and are listed below:

- The OS must be protected from user processes
- The users must be protected from each other
- The users must be protected from themselves
- The OS must be protected from itself
- The OS and resources must be protected from environmental failures

To ensure that the OS remains reliable and the integrity of the OS is not compromised, it is crucial to define adequate controls and ensure that they are implemented, verified, tested, and maintained properly. Ensuring that the above goals of an OS are not violated, is the task of OS security.

OS Security Checklist

As discussed before, OS is a crucial component of an IS and is the interface that users have, with the infrastructure. So, it plays a very important role and should be controlled effectively, to control other components of the IS.

This section describes a probable security checklist, to harden an OS and to provide a basis for a secure OS installation.

It should be noted that, depending on the configuration of the IS, viz. stand-alone and networked, and the size of the IS network, the risks and focus areas of control also vary. This section identifies, some of the common focus areas for strengthening a single host OS in a networked environment.

Focus on OS strengthening (hardening) is not only a post-installation effort, but starts even before the OS is installed. This section looks at the following focus areas:

- Pre-installation
- Installation
- Post-installation

Pre-installation Checklist

Even before the installation of an OS, care should be taken to ensure that the choice of the OS, suits the need of the IS. Apart from this, all OSs come with some basic configurations, which in most cases, are not secure. So, focus has to be laid on understanding the pre-configured status of the OS, in terms of security threats. It is also vital for the administrator to understand all the installation parameters.

It was found in various surveys that the predominant area of attack, on a system involved, predefined user accounts, configurations which the vendor included, but were not changed or disabled by the installer, etc.

This section, describes a checklist for identifying risk factors in an OS, before installing it.

- Will the system be networked?
- Is the system multi-boot?
- Will the system be multi-homed?
- What services need to be provided by the system?
- What is the configuration of the system?
- What devices should be allowed or disabled?
- Are the BIOS settings, secure?

- What accounts are provided by default, by the vendor?
- What resources are accessible by default, for all users?

Installation Checklist

Most of the features allowed by the OS, are typically configured during the installation process and hence, care should be taken, during the installation process, to ensure that the system is secure, right from the stage of installation. Any lacunae in the default security, settings, as provided by the vendor, will be corrected in the next (post-installation) stage.

This section, describes a checklist for the installation process.

- Install minimal OS configuration
- Ensure that latest security and other patches, provided by the vendor are installed
- Secure BIOS settings
- Restrict application search path and access to the system directories
- Uninstall/ disable all services that are not required
- Avoid typical installation
- Disable the default accounts and resources, provided by the vendor, unless approved in the pre-installation checklist.

Post-installation Checklist

Once the OS is installed, hardening of the OS is very important and different areas of the OS should be protected. This section, describes a basic OS hardening checklist, for usage after installation of the OS.

User Accounts

- Since the most common way of accessing an OS and its resources is through user accounts, care should be taken to ensure that unused user accounts are disabled, default (vendor-created) user accounts are modified adequately, to ensure that the default passwords are at least modified. Ignoring the default user accounts, is a major, first point of attack on many OSs.
- Ensure that all user accounts, need a password to access the system, that a secure password management policy exists and relevant procedures for the same are available and used without fail
- Ensure that the need to use the super user account is minimized, by ensuring that different roles in the IS are mapped to user groups in the OS, and users belonging to these groups have access, only to the

relevant resources. For example, if an OS has a database (DB) server, access to the DB files should be available only through the DB interface and even the super user, should not have a reason to handle these DB files, directly. This ensures accountability in the system, ensuring that any inconsistencies in the DB system are the responsibility of the DB administrator only. So, ensuring that the super user account is used minimally, is crucial.

Network Access

Most systems in the current environment are networked and there should be enough controls to ensure that access to resources, on the network is also controlled. In a networked environment, network controls play an important role, but weaknesses in the OS controls could circumvent any strong network controls. So, access to network resources, should be securely controlled, even at the OS level and the OS should not allow access to network resources, beyond what is/should be allowed.

System Auditing

All crucial aspects of computing on the IS, should be audited regularly and important user accounts and it is mandatory for resource access to be logged securely, in logs that can be audited at a later stage.

It is crucial that access to these logs be secured, to ensure that any intruder in the system, cannot modify these logs, to cover up the intrusion.

System Services

Apart from uncontrolled, vendor-provided user accounts, being the most frequently-used mechanism to commit security breaches; unnecessary services, available on the system, are the second-most important points of attack, by attackers. As part of the pre-installation checklist, it was suggested that the exact services that the system would provide, be identified and only these services be installed, during the installation phase. This is a very crucial aspect of OS security and if neglected, could become a major threat to the integrity of the system.

For example, even a normal desktop machine, used from home, could be attacked, if accessing the Internet through unnecessary services, running on the system.

It is strongly suggested that OS installation be minimal, i.e. an OS installation that contains components required for a specific task. For example if the system is expected to be used as a web server, only the web server components should be installed and that there be a continuous process to

ensure that unnecessary services are disabled. Importantly, those services that are enabled, (because they are necessary) should have adequate controls and audit mechanisms, to check for intrusions.

CONSOLIDATED CHECKLIST

Table 8.4

<i>S. No.</i>	<i>Installation Phase</i>	<i>Item</i>	<i>Description</i>	<i>Suggestion</i>
1.	Pre-installation	What is the system configuration?	Understanding the system and available resources is crucial to ensuring that all points of possible attack are identified.	Recommended
2.	Pre-installation	Are the BIOS settings, secured by a password?	Ensuring that the BIOS settings are secured by a secure password, is crucial to ensure that boot-up sequences are not circumvented.	Mandatory
3.	Pre-installation	Complete device list, with 'need to enable/disable' status.	Identification of all the devices available ensuring that and only those resources that should be enabled are actually enabled.	Mandatory
4.	Pre-installation	Is the system multi-boot?	Now with more, and more-state-of-the art tools available, having multi-boot machines, ensures that files in one OS partition can be accessed by other OS tools, thereby circumventing inherent security controls in the OS. So, for secure systems, multi-boot should not be allowed.	Mandatory

(Contd)

<i>S. No.</i>	<i>Installation Phase</i>	<i>Item</i>	<i>Description</i>	<i>Suggestion</i>
5.	Pre-installation	Is the system networked?	Networking a system, increases multifold, the threat to the system and extra care should be taken to ensure that even over the network, the system is not compromised and at the same time the system does not compromise the security of other systems on the network.	Recommended
6.	Pre-installation	List of user accounts and default access controls, configured by the vendor.	The OS vendor, typically, builds the system for novice users and provides various default user accounts and access privileges. Before installation, it is important to understand what these accounts are, to ensure that they are secured, adequately.	Mandatory
7.	Pre-installation	What are the resources, available by default to all users (as configured by the vendor)?	Apart from default user accounts, vendors also set default resource access privileges, which could be contrary to the IS policies. So, before installation, we should keep track of these and ensure that the access privileges are in accordance with the organization's IS policies.	Mandatory
8.	Installation	Install custom OS configuration.	For security reasons, do not employ typical or complete installation of the OS.	Mandatory

(Contd)

404 Information System Audit and Assurance

<i>S. No.</i>	<i>Installation Phase</i>	<i>Item</i>	<i>Description</i>	<i>Suggestion</i>
9.	Installation	Ensure that the latest security patches are installed.	Ensure latest security patches are tracked and installed, without fail.	Mandatory
10.	Installation	Secure the BIOS settings.	Secure the BIOS settings to ensure that a user, at a later stage, cannot circumvent the boot controls.	Mandatory
11.	Installation	Uninstall/disable all services that are not required.	Only those services that have been identified during the pre-installation checklist should be installed.	Mandatory
12.	Post-installation	Restrict access to system directories and application search path, to normal users.	Only super/power users should be able to access the system directories.	Recommended
13.	Post-installation	Uninstall/disable all services that are not required.	Only those services that are required should be allowed on the system.	Recommended
14.	Post-installation	Ensure that all users have password access.	There should not be any users without passwords.	Recommended
15.	Post-Installation	Ensure that all default passwords, provided by the vendor, are modified.	Default user accounts with unmodified default passwords are the predominant, first points of attack, on any system. So, this conduit should be shut down, without fail.	Mandatory

(Contd)

<i>S. No.</i>	<i>Installation Phase</i>	<i>Item</i>	<i>Description</i>	<i>Suggestion</i>
16.	Post-installation	Ensure that the super user account is used minimally.	Though contradictory to most common practices, ensuring that super user account is used minimally and all super user activity is logged and audited, is a secure practice.	Mandatory
17.	Post-installation	Define user groups for different IS roles and assign the users these roles and define access controls for these roles.	This very critical for secure systems, and more importantly, for accountability in the system.	Recommended
18.	Post-installation	According to the location of in the system the networked IS, ensure that access to resources on this system, through the network, is controlled.	We should ensure that apart from system controls for security, the security of the system is not compromised over the network.	Mandatory
19.	Post-installation	Ensure that the system does not pose a threat to other resources on the network.	Ensure that adequate controls exist, to check insecure access to network resources from this system.	Recommended

(Contd)

406 *Information System Audit and Assurance*

<i>S. No.</i>	<i>Installation Phase</i>	<i>Item</i>	<i>Description</i>	<i>Suggestion</i>
20.	Post-installation	Ensure that access to audit logs is secure and users cannot modify them, after they are created.	Ensuring that logs created are secured, is an important requirement for effective audit and intrusion detection.	Mandatory
21.	Post-installation	Audit log formats should be effective and tools should be used to track inconsistencies in the log.	There are a lot of systems available, which track log files and provide automated audit reports. These should be used to augment the manual audit procedures.	Recommended
22.	Post-installation	Deployment of IDS systems to ensure that any possible intrusion activity is detected.	Automated tools like IDS and other services, provide an effective tool to the security administrator, to understand the security of the system.	Recommended

LINUX SECURITY CHECKLIST

This section describes some of the common security checklist elements for the Linux OS. These are only indicative and do not form a complete list of elements. The exact list can be derived from this list, based on specific installation and implementation requirements.

Table 8.5

<i>S.No.</i>	<i>Installation Phase</i>	<i>Description</i>	<i>Priority</i>
1.	Pre-installation	Identify minimum OS packages.	Mandatory
2.	Pre-installation	Get the latest security and feature patches for the OS and different applications/services, selected.	Mandatory
3.	Pre-installation	Set a Bios password.	Mandatory
4.	Pre-installation	Set a LILO/GRUB password.	Mandatory
5.	Installation	Disable root login.	Mandatory
6.	Installation	Disable telnet service and use ssh instead.	Recommended
7.	Post-installation	Set up user path to include only protected directories.	Recommended
8.	Post-installation	Check files that are loaded during root login sequence.	Mandatory
9.	Post-installation	Disable default trusted host configurations by modifying the /etc/host.equiv or .rhosts files.	Mandatory
10.	Installation	Do not install any clients (telnet, ssh client or others) on the server. This ensures that breaches are that much more difficult to achieve.	Recommended
11.	Post-installation	Ensure that all user accounts require passwords.	Mandatory
12.	Post-installation	Disable all unused/unnecessary user accounts. During installation, a host of user accounts like, adm, bin, daemon, ftp, games, halt, ident, listen, lp, mail, mysql, named, news, nobody, operator, noaccess, shutdown, uucp, etc. are created by default. These should be disabled, unless there is a strong reason not to.	Recommended
13.	Post-installation	Ensure that passwords are at least 8 characters long.	Mandatory

(Contd)

408 *Information System Audit and Assurance*

<i>S.No.</i>	<i>Installation Phase</i>	<i>Description</i>	<i>Priority</i>
14.	Post-installation	Device a password policy with lifecycle, and other parameters for better password management.	Recommended
15.	Post-installation	Review user accounts, for accounts with 0 uid.	Mandatory
16.	Post-installation	Ensure that shadow passwords are used and all accounts have an 'x' in the password field in /etc/passwd file.	Mandatory
17.	Post-installation	Ensure that /etc/shadow file has "*" in the password field, for all user accounts that are disabled.	Mandatory
18.	Post-installation	Use tools like, sudo for better role-based control and granularity of access and better accountability.	Highly recommended
19.	Post-installation	Remove all unneeded services from the startup scripts.	Mandatory
20.	Post-installation	Ensure that setuid programs are documented and ensure that only standard programs, introduced through a documented process are allowed for setuid privileges.	Mandatory
21.	Post-installation	Ensure that the umask is set properly for the root and other users.	Mandatory
22.	Post-installation	Install and configure firewalls, to ensure security from and to the other network resources.	Recommended
23.	Post Installation	Ensure that all server log files are secure and normal users cannot view/modify these files.	Mandatory
24.	Installation	Disable X on servers and ensure that if any ui-based configuration is required, web interfaces or linuxconf is used, instead of the gui configuration tools, available with X windows.	Mandatory
25.	Post-installation	Log all the su activity.	Mandatory

CHECKLIST FOR WIN2K**Table 8.6**

<i>S.No.</i>	<i>Type</i>	<i>Description</i>	<i>Priority</i>
1.	Installation	Ensure that the latest hotfixes and service packs are installed.	Mandatory
2.	Installation	Ensure that all drives are NTFS in settings/control panel/administrative tools/computer management/storage/disk management. Ensure that the correct permissions are allocated to sensitive data and application files and folders.	Mandatory
3.	Post-installation	Ascertain if a security template is being used. Ensure that the hisec*.inf template is used. The template used, depends on the circumstances of the environment, e.g. notssid.inf template is used in instances, where older programs are run on a terminal server. The templates and their system uses are as follows: • basicwk.inf: Default workstation • basicsv.inf: Default server • basicdc.inf: Default domain controller • compatws.inf: Compatible workstation or server • notssid.inf: Terminal services backward compatibility • securews.inf: Secure workstation or server • hisecws.inf: Highly secure workstation or server • securedc.inf: Secure domain controller • hisecdc.inf: Highly secure domain controller If changes to the template have been made, ascertain if the changes are plausible. Determine how often security analysis is performed and what steps are taken to correct the security weaknesses. Ensure that the template is stored on a CD or floppy.	Recommended

(Contd)

410 Information System Audit and Assurance

S.No.	Type	Description	Priority
4.	Post-installation	Ensure that a baseline analysis is maintained, to ascertain the progress made in security configuration. Security analysis: • Run the security analysis, • Start/run/type mmc/ok. On the console menu, choose add/remove snap-in, • In the snap-in window, choose add, choose security configuration and analysis and click on add. Right click on security configuration and analysis, open database, type in a name for the database and click on open. In the import template window, select the hisecdc.inf template and click on open. Again, the template needs to match the circumstances of the environment. • Right click security configuration and analysis and select 'perform analysis now' and then click on ok. • You can then, either review the results at the default location or alternatively export it in text format.	Recommended
5.	Post-installation	Account policies: ensure that at a minimum, the following settings are present: • Password policy 1. Password history = 5 previous passwords, 2. Maximum password age = 30 days, 3. Minimum password age = 1 day, 4. Minimum password length = 8 characters, 5. Password must meet complexity requirements = enabled, 6. Store passwords, using reversible encryption = disabled. • Account lockout 1. Account is lockedout, until the administrator unlocks it,	Recommended

(Contd)

S.No.	Type	Description	Priority
		2. Account lockout threshold = 3 invalid passwords,	
		3. Reset account lockout counter after 30 minutes,	
		4. Local policies. Recommended	
		• Audit policy	Recommended
		1. Audit account logon events— Success and failure.	
		2. Audit account management— Success and failure.	
		3. Audit directory service access— Success and failure.	
		4. Audit logon events— Success and failure.	
		5. Audit object access— Success and failure.	
		6. Audit policy changes— Success and failure.	
		7. Audit privilege use— Success and failure.	
		8. Audit process tracking— Success and failure.	
		9. Audit system events— Success and failure.	
		• User rights	
		1. Act as part of the operating system: Disable.	
		2. Add workstations to the domain: Restrict to system administrator.	
		3. Backup files and directories: Res- trict to backup operators.	
		4. Change the system time: Disable and restrict to system administrator.	
		5. Create a token object: Restrict to system administrator.	
		6. Create permanent shared objects: Restrict to system administrators.	
		7. Debug programs: Restrict to developers and system adminis- trators.	
		8. Deny logon as a batch job: Enable.	

(Contd)

412 Information System Audit and Assurance

S.No.	Type	Description	Priority
9.		Deny logon as a service: Enable.	
10.		Force shutdown from a remote system: Disable.	
11.		Generate security audits: Enable.	
12.		Increase scheduling priority: Restrict to system administrator.	
13.		Load and unload device drivers: Restrict to system administrator.	
14.		Lock pages in memory: Restrict to system administrator.	
15.		Logon as a batch job: Disable.	
16.		Logon as a service: Disable.	
17.		Manage auditing and security log: Restrict to system administrator	
18.		Restore files and directories: Restrict to system administrators and back-up operators.	
19.		Shutdown the system: Restrict to system administrators.	
20.		Synchronise directory service data: Restrict to system administrator.	
21.		Take ownership of files or other objects: Restrict to system administrator.	
• Security options			
1.		Allow server operators to schedule tasks (domain controllers only): Restrict to server operators and system administrators.	
2.		Allow systems to be shutdown without having to logon: Disable.	
3.		Allow ejection of removable NTFS media: Restrict to system administrator.	
4.		Amount of idle time allowed before disconnecting a session: Maximum, 2 hours.	
5.		Audit the access of global system objects: Enable.	
6.		Audit use of backup and restore privilege: Enable.	

(Contd)

S.No.	Type	Description	Priority
7.		Automatically log off users when logon time expires (local): Enable.	
8.		Clear virtual memory pagefile, when system shuts down: Enable.	
9.		Disable CTRL+ALT+DEL requirement for logon: Disable, if using smart cards.	
10.		Don't display last username in logon screen: Enable.	
11.		LAN manager authentication level: Should be NTLMv2.	
12.		Message text for users, attempting to logon: Enabled with the legal notice.	
13.		Message title for users, attempting to logon: Enabled with WARNING title.	
14.		Number of previous logons to cache, in case of domain controllers not being available.	
15.		Prevent system maintenance of computer account password: Enabled.	
16.		Prevent users from installing print drivers: Enabled.	
17.		Prompt user to change password before expiry: Should be about 14 days.	
18.		Recovery console: Allow automatic administrative logon: Disable.	
19.		Recovery console: Allow floppy copy and access to all drives and all folders: Restrict to system administrator.	
20.		Rename administrator account: Enabled.	
21.		Rename guest account: Enabled.	
22.		Restrict CD ROM access to locally logged on user only: Enabled.	
23.		Restrict floppy access to locally logged on user only: Enabled.	

(Contd)

414 Information System Audit and Assurance

S.No.	Type	Description	Priority
24.		Secure channel: Require strong (Windows 2000 or later) session key: Enabled.	
25.		Shutdown system immediately if unable to log security audits: Enabled	
26.		Strengthen default permissions of global system objects, e.g. symbolic links: Enabled.	
		• Event log	Mandatory
1.		Maximum log size for application, security and system log: This has to be a minimum of 2 MB.	
2.		Restrict guest access to the application, security and system log = enabled.	
3.		Retain application, security and system log: Should be in terms of the security policy.	
4.		Retention method for the application, security and system log should be clearly documented.	
5.		Shutdown the computer when the audit log is full: enabled.	
		• Restricted groups	Recommended
1.		Administrators: Ensure that only authorized users are members of this group.	
2.		Backup operators: Ensure that only authorized users are members of this group.	
3.		Guests: Ensure that no one is a member of this group.	
4.		Power users: Ensure that no one is a member of this group.	
5.		Replicator: Ensure that no one is a member of this group.	
6.		Users: Ensure that only authorized users are member of this group.	

(Contd)

S.No.	Type	Description	Priority
		• System services Ensure that only those services, which are necessary for the server to perform its function, are enabled. All other services, must be disabled. View the security relating to each enabled security element and ensure that only the administrator has full access, to enable a service. The following services should be disabled: 1. Remote registry service, 2. Telnet, 3. Alerter, 4. Server, 5. Messenger, 6. SNMP.	Mandatory
		• Registry Ensure that the following requirements are met with: 1. Legal notice: Enabled, 2. Don't display last username, 3. Disable caching of logons, 4. Disable floppy drives and hide drive letters, 5. Print drivers are secured, 6. Crash control enabled with logging to event log, dumping of file, no auto-booting, send an alert and do not overwrite. 7. Permissions on winreg key should be set to full access, to system administrators and system accounts only. 8. Disable crash, on audit failure. 9. Restrict anonymous access. 10. Enable full privilege auditing. 11. The permissions on the registry should be restricted to full access, to the administrator and system accounts.	Mandatory

SUMMARY

In this chapter, we discussed different kinds of system configurations that are normally found and the type of operating systems that are used in these configurations. We then identified various functional components, viz. process management, memory management, file system management, I/O management, network management, and protection system and the various services they offer. In the context of different services that are offered, the operating system faces different kinds of threats and we looked at the concepts of hardening or securing the operating system against these threats. We also discussed the role of the utility software and threats that emanate from using such software, bypassing the deployed controls. We then looked at OS controls at three levels, viz. pre-installation, Installation and post-installation controls and outlined a generic security checklist in this context. At the end, for the convenience of the auditors, we also provided the security/audit checklist for Linux and Windows 2000.

REVIEW QUESTIONS

1. What are the different kind of operating system and how are these used in various system configurations?
2. Describe the different functional components of operating systems and the services they offer.
3. Describe the process management function of an operating system and differentiate between co-operative and pre-emptive process management.
4. Discuss the file system organization and the advantages of using a hierarchical directory structure.
5. What is a protection system and how do we use domains to control the access to resources?

MULTIPLE CHOICE QUESTIONS

1. For selection of appropriate operating system software for the organization, more stress should be given to:
 - (a) Security provided by the operating system
 - (b) Hardware compatibility
 - (c) Inter-operability of the OS
 - (d) The vendor's reputation in supplying the OS
 - (e) User approval

2. Which of the following is most appropriate for hardening of OS?
 - (a) Removing the resource-hungry services from the OS
 - (b) Only using the vendor-recommended services
 - (c) Removing unnecessary services
 - (d) Enabling only those services that are planned and required
3. Which of the following is most likely, the goal of a reliable operating system:
 - (a) OS must be protected from itself
 - (b) OS must protect user processes from themselves
 - (c) OS must protect user processes from each other
 - (d) OS must protect the environment from user processes
4. Which of the following statements, best describes multi-processing?
 - (a) Ability of the OS to allow multiple-users to execute programs simultaneously
 - (b) Ability of the OS to allow multiple-users to execute multiple-programs simultaneously
 - (c) Ability of the OS to switch multiple-programs, at a very high speed
 - (d) Ability of the OS to execute multiple-programs simultaneously
5. Which of the following statements about utility software, is incorrect?
 - (a) Utility software are add-ons to the operating system
 - (b) Utility software allow the user to perform diagnostics on the system
 - (c) Utility software can circumvent the access controls
 - (d) Utility software are generally OS-specific
6. Which of the following statements about the directory organization, is the most correct?
 - (a) All OSs, use the same kind of layout for files, in a directory structure.
 - (b) All OSs, allow a graph layout of the directory structure
 - (c) Directory structures are hierarchical in nature
 - (d) Files in a directory structure can be shared independently
7. When installing a patch in the OS the most important concern for the organization is:
 - (a) Untested patches
 - (b) New problems associated with a patch
 - (c) System down time
 - (d) Integrity of the patch

418 *Information System Audit and Assurance*

8. The large number of easily accessible tertiary storage I/O devices:
 - (a) Are a serious threat to security on the system
 - (b) Enable backup/restore services, to help them become more efficient
 - (c) Degrade the performance of the OS
 - (d) Allow users to manage data on their system, without burdening the administrator
9. Which of the following is a pre-installation security requirement for an OS?
 - (a) Ensuring that logs are maintained securely
 - (b) Ensuring that users belonging to various groups are identified
 - (c) Identifying the default vendor configurations
 - (d) Identifying the requirement for the applications.
10. While conducting an OS review, which of the following should be given importance by the auditor?
 - (a) The requirements of the user
 - (b) System down time
 - (c) Ability of the user to install programs
 - (d) Baseline configuration of the OS

DISCUSSIONS AND RESEARCH QUESTIONS

1. 'Operating system control is more about providing controls to ensure that controls in other subsystems are not compromised due to access violation'. Discuss.
2. 'Utility software are the weak link in the system security chain'. Discuss.
3. 'The user interface services are important to increase user acceptance of the operating system. Discuss.
4. 'Program installation/uninstallation services, play an important role in popularizing the operating system usage with many applications'. Discuss.
5. Discuss the importance of understanding the threats of vendor-provided default configuration to the OS.
6. Discuss the threats of multi-boot or multiple operating systems, on the same machine.

EXERCISES

1. Define an access matrix for the protection system of an OS, installed to be used as a web server for launching Internet banking.

2. Draw the system configuration for your organization, identifying the various kinds of OSs that will be used in different components of IS.
3. Write a checklist for hardening your E-Mail server (Microsoft Exchange 2000).
4. Identify the various threats to IS, where different OSs coexist.
5. Identify a pre-installation checklist for hardening a Linux system, to be used as PDC (Primary Domain Controller).

9

Operational Control Review

-
-
- ❖ Operation management—The IS engine
 - ❖ The functional areas of computer operations
 - ❖ Light out operation
 - ❖ System and network administrator
 - ❖ Control requirement for backup
 - ❖ Scheduling
 - ❖ Controlling input/output operation
 - ❖ Documentation and program library
 - ❖ Controls relating to removable storage media
 - ❖ Technical support and help desk
 - ❖ Quality assurance
 - ❖ Physical and environmental security
 - ❖ COBIT and operational control
 - ❖ Operational risk from a banking perspective
 - ❖ Audit checklist
-
-

OPERATION MANAGEMENT—THE IS ENGINE

Whatever be the controls, in the application, database management system and operating system, operational controls are very important for an organization, as these controls act as a limiting factor, for all other controls. For example, an application system, with all the relevant controls, will not be effective, if the operations group does not take the backup, regularly. Given the criticality of the Information System in many organizations, operation management is considered to be, the engine of the Information System in an

organization, which drives the entire organization towards fulfilling its business objectives. The tasks that operation management performs, may be very simple and straightforward, but these are nonetheless, critical to the success of the organization. A significant transformation has taken place, happened in the way the operational functions are exercised in the organizations. Some of the noteworthy changes, which have control implications are outlined below:

- Many operations which were manual, are now, automated. As a result, the authenticity, accuracy and completeness of actions, undertaken by the operation personnel, are now, relegated to the automated systems,
- Change in the setup, i.e. from a centralized to a decentralized environment, or vice versa. In fact, in the banking and financial sector, all over the world today, the pattern reflects a change from decentralized operations to centralized operations.
- The cost of the hardware has become relatively low. So, efficiency of the components, is no more an issue. On the other hand however, the demands of the users, have increased manifold, in terms of performance expectation. Therefore, the Service Level Agreement, between the users and the operation group, has become very important.
- There is a growing move, towards outsourcing the operation functions, because it allows economy of scale and helps the organization, concentrate on and specialize in its core activities.

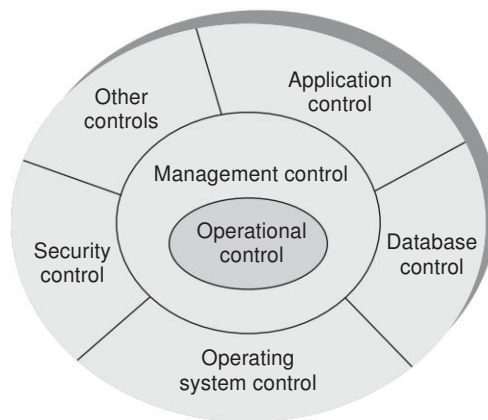


Fig. 9.1 Operational control—the core

THE FUNCTIONAL AREAS OF COMPUTER OPERATION MANAGEMENT

Although the functional areas of computer operation will vary, from one organization to another, depending on the size of the computer installation, workload, number of work areas that are computerized, type of IS, i.e. centralized or distributed, and moreover the dependencies of the organization on computers; the Information System operation, generally, includes the following functional areas:

- Computer operations and management
- Scheduling
- Controlling input/output function
- Documentation and program library
- Control over consumables
- Technical support/helpdesk
- Software maintenance
- Quality assurance

Computer Operations and Management

Computer operations, essentially involve, providing the necessary support for running the applications or programs. This includes inter alia, starting the program, loading the media, managing output devices like, printers, observing the information processing facility for unauthorized entry, backup and restore, and routine health check-up of the servers/routers/firewall, etc. All these operations, mentioned above, are undertaken centrally, at one place, or at distributed locations, depending on the application architecture, organization's architecture and above all, the network connectivity across the organization. The operational control issues, related to centralized IS operation vis-à-vis distributed IS operations, are mentioned in Table 9.1.

Table 9.1 Centralized vs. distributed operation

<i>Centralized operation</i>	<i>Distributed operation</i>
1. The operation cost, as well as the cost of hardware and software, would be comparatively less, due to economies of scale.	1. Although the operational cost and the cost of the hardware and software, would be comparatively more, the difference is decreasing because of a gradual reduction in the cost of computing.

(Contd)

<i>Centralized operation</i>	<i>Distributed operation</i>
2. Management control, over the operations will be more effective, as it will be confined to one location.	2. Management control will be difficult, due to diverse locations.
3. Easy and convenient, change management.	3. Change management becomes difficult, due to diverse locations.
4. Easier troubleshooting, as it can be done centrally.	4. Troubleshooting becomes difficult, as it becomes difficult to find the problem and shoot it in a distributed environment.
5. Susceptible to single point of failure.	5. Failure at one point, will affect, only a specific area and not the entire organization.
6. Concentration of resources, including the IS expertise, at one place. Thus, there is a need for rotation of staff.	6. IS expertise is distributed.
7. Problems in sizing of the IS resources, viz. DB server, etc., which may affect the efficiency.	7. Sizing of the servers and bandwidth issues, are not major issues.
8. Easier to have varied delivery channels.	8. Difficult to implement security policy.
9. Easier to implement security policy.	9. Lack of homogeneity across the organization.
10. Easy to have effective Management Information System (MIS).	

Whatever be the operational control architecture, whether centralized or distributed, there are certain operational controls, viz. physical access controls, etc. which can only be implemented onsite.

Operational control activities can also be performed by Automated Operations Facility (AOF), popularly called 'light-out' operations. Although, traditional controls like, separation of duties and controls, related to the safety of human lives, are not quite required for a light-out facility, the management should nonetheless, take care of the authenticity, accuracy and completeness of the automated operations. The following control issues are very important for the purpose.

- The design, implementation and maintenance of the parameters, set out in the light-out facility, i.e. when should the system start a particular process, what media should be loaded?, etc. The basic questions, the auditor should focus on, are who authorizes these parameters? Are there any change management procedures for bringing about changes in the parameters?, etc.,
- The standards for the design and implementation of the parameters, for the light-out operations or Automated Operation Facility (AOF),
- The integrity of the parameter file,
- The change management procedure, for maintaining the parameter file,
- Backup procedure of the parameter files.

Advantages and Disadvantages of Light-Out Operation

Advantages

- Human errors and oversights can be avoided,
- The issues relating to the management of personnel, are also reduced,
- The work of the Information System Area, is also reduced,
- Cost containment,
- Continuous, uninterrupted operation,
- Reduced number of system errors and interruptions.

Disadvantages

- In the event that the AOF fails and human intervention is required, the operations staff may no longer have the knowledge and experience, needed to sustain operations in the manual mode,
- Very difficult to have a generic parameter. A slight change in the hardware and software, makes the parameter inoperable and it may not be possible to carry out these modifications quickly, particularly, in times of stress,
- Rapid change in the technology, makes the technology in vogue, obsolete,
- The cost of setting up of AOF facility, sometimes becomes prohibitive,
- It may happen that the AOF does not support all the computer operations of the Information System. In this case, some parts of the activities are operated manually and some parts are automated.

Such kind of a diverse environment, requires a diverse audit approach. The IS auditor's role in this kind of an environment, is not only to evaluate the automated control or the manual control, but also, the interfaces between these two. Another kind of diverse environment is the centralized operation, where major automated computer operations (backup, etc.) take place; while at the client's site, there are microcomputers, having hard disks, which also process and store some information, but these operations are performed manually. In such cases, auditors must consider the need for operation controls, across all hardware/software platforms.

For collecting evidence, on the quality of computer operations, the auditor should examine various documents, viz. hardware error report, availability report, utilization report, etc. and should also undertake interviews, with the operation management personnel. Observation of the activities of the operation personnel, will enable the auditor to take a view on documented policies, procedures and practices.

Hardware Error Reports

Indicate failures/malfunctioning, related to CPU, input/output, and power and storage failure. This report should be viewed by the IS operation management, to take corrective actions.

Availability Reports

These reports indicate the availability of the computer operation, for the intended users. These reports will also address the issue of IS inactivity, referred to as 'downtime'. The IS operation management should review this report and find out the reasons for such inactivity, which could be due to various factors, viz. hardware failure, software failure, environmental failure (power supply, air-conditioning, etc.) and take corrective action.

Utilization Reports

Such utilization reports, document the utilization of hardware, software and peripherals. Software monitors are used, to capture the utilization of processors, channels and secondary storage devices. IS operations can parameterize the thresholds, as per the business requirement and vendor's specifications, and take remedial actions.

Considering the various important activities which comprise the IS operation, three broad roles are very important, viz. system administration,

database administration and network administration. From a security and control perspective, all these three activities, should be separated, to avoid role conflict. The activities performed, for these functions are as follows.

SYSTEM ADMINISTRATION

The work of system administration, essentially involves, the activities relating to maintenance and upkeep of the hardware and system software, particularly, the operating system. The various functions that are associated with system administration are as follows:

- Adding and configuring new personal computer/workstations
- Installing system software
- Creating, issuing, deactivating, reinitializing, and monitoring user IDs and associated passwords
- Defining user groups and associated resource access control profiles
- Implementing procedures to remove/prevent the spread of viruses and other unauthorized software
- Allocating storage space for users in systems
- Maintaining logs on individual systems
- Ensuring the physical safety of the systems
- Ensuring the proper storage of licenses, manuals, etc. and prompt retrieval of these
- Sharing administrative privileges
- Ensuring confidentiality of both the system passwords
- Ensuring that no unauthorized person has access to system passwords
- Ensuring that an administrator-equivalent password is maintained and held by another official, in case of emergency,
- Backup and restoration, etc.
- Change management

NETWORK ADMINISTRATION

The work of the network administration, involves all aspects of the network, including designing, planning, configuration, installation, troubleshooting and maintenance.

The important activities to be performed by the network administrator, can be classified as follows.

Maintenance of Network

The network administrator should:

- Monitor servers' power supply and the UPS,
- Monitor the backup facility/log,
- Monitor network performance,
- Perform routine virus scan/ detection/ removal, at the entry point of the network,
- Monitor user backup activity,
- Perform routine network maintenance,
- Install, maintain and update software and hardware,
- Maintain network applications,
- Maintain network hardware and cabling,
- Maintain disaster prevention/ recovery procedures.

Change Management

The network administrator should:

- Evaluate the impact of network changes and additions,
- Review and approve all planned network changes and updates.

Disaster Prevention/Recovery

The network administrator should:

- Perform network/general disaster, recovery drills,
- Modify disaster prevention procedures, as and when needed/ necessitated,
- Schedule downtime and notify all users, sufficiently, in advance,
- Monitor and inform the users of the status of the network, in case of downtime.

Reporting

- If any undesired/ illegal activity is noticed during the monitoring of logs, the administrator should report the matter, immediately, to the authorities, for appropriate follow up action,

- Apart from the above-mentioned reporting, there should be a regular, monthly report, made by the network administrator and submitted to the IT management.

Miscellaneous

- Follow up with vendors, over purchase and installation of equipment,
- Verification of received material, so as to conform to the policy requirements, of the organization,
- Liaise with service providers, during any network downtime and ensure speedy recovery.

Note that the network administrator, should never have to perform any application or programming tasks, although he/she is also a normal user of the Information System.

DATABASE ADMINISTRATION

The tasks of the database administration include, the design, definition and proper maintenance of the corporate database. Some of the important activities of the database administrator are as follows:

- Specifying the physical data definition,
- Changing the physical data definition, to improve performance,
- Selecting and implementing, database optimization tools,
- Testing and evaluating the programmer and optimization tools,
- Implementing various controls in the database management system, viz. definition controls, access controls, update controls and concurrency controls,
- Monitoring database usage, collecting performance statistics and tuning the database,
- Backup and recovery of database.

In case of banking industries all over the world, the shift is towards centralized operations, popularly referred to as, core banking solutions. In case of such solutions, most of the IS operations are carried out from a centralized data centre. Although the management overheads of computer operation, are reduced because of the centralized operation, the risk level of the IS also increases, as failure or malfunctioning at the data center, will affect the entire organization. Therefore, the management should take necessary steps,

for separation of duties, job rotation and framing appropriate policy, procedures and job cards, for various functionaries, at the data centre. Documented procedures are required for important activities like, backup/restoration and also, for infrequent activities like, system crash, etc. Separation of duties at the data center, will give the malicious operator, fewer opportunities for perpetuating illegal activities.

Considering the importance of backup in a centralized operation environment, some extra inputs for backup policy have been discussed below, which will be useful, in developing the appropriate backup policy and procedures.

CONTROL REQUIREMENTS FOR BACKUP

- All computer systems and their associated data files, should have, agreed and documented backup and recovery (restoration) procedures, for their associated data files
- The most recent backup tapes or disks, must be stored in a secure environment, e.g. a fireproof cabinet, with regular transfers, to and from remote (off-site) storage
- Backup of software (both, application and system software) and configuration files, should be taken regularly, and protected carefully. Additional backup should be taken, as soon as there are updates or version changes, to the software
- All data files and their associated software programs, relating to core activities should be retained, as per the business needs and must be kept secure
- The organization should ensure that access to the 'old' data is available, whenever required, which can be achieved by archiving to optical disks/CDs
- Periodicity of the backup should be decided, depending upon the criticality of the data
- Front office application data, like that of branch operations, need to be backed up, not only daily, but also, more than once (multiple copies)
- Backup should be viewed primarily, as a disaster recovery mechanism and appropriate significance must be attached to it
- Full backup or milestone backup should be taken once a quarter, usually, on the last day of the quarter. This should be stored offsite or archived or copied to appropriate media

- Separate guidelines should be framed, for backing up critical and non-critical data
- Backup does not necessarily mean, that which is on tapes/ CDs. In the present day scenario, where hard disks are cheap, hard disk backup must be considered, since it is fast and easy

ARCHIVING

This is applicable to information, which is not required on a day-to-day basis, but which needs to be retained for a long period, and is also applicable to information, which is retained in perpetuity and referred to, infrequently, but periodically. Such data is often removed from the day-to-day processing area, thereby, reducing the overheads on storage and processing resources.

Weaknesses in the longevity of the media, used for archives, can result in a failure to restore the required data, when eventually, it is needed. Archived data can often be retained in a proprietary format, which is no longer supported by the present systems, thus, hampering attempts at access. These are the concerns, to be addressed, while backing up the data, for archival purpose.

OFF-SITE BACKUPS

To ensure the availability of and access to, the data files, following a disaster, copies of the files must be stored in a location, separate from where the data files are normally, preserved. This off-site storage is applicable to data files, which are used on a regular basis, in conducting business, as well as those, which must be retained, to meet the requirements of the legislation and other regulations, in force, regarding retention of records.

Information security and corporate security, should review existing and potential off-site storage facilities, to determine the protection, which should be provided, to the data, stored at such locations. This review should address environmental, physical and procedural security issues, directly related to the facility, handling and movement of the media.

There should be a system for having taking off-site storage of all backup media, as well as, entrusting the responsibility for regular preservation of the off-site backup media, by framing appropriate procedures.

STORAGE OF BACKUPS

Finding a good way to store backups, is almost as important, as creating them. Backups, installation media and boot disks, should be stored in a place, where

only authorized people have access to them. In order to make restorations simple, backups need to be well-labelled. Labelling includes, clearly marking the media itself, as well as, including a table of contents, so that individual files on the tape, can be located easily. In sites, where several people share the responsibility of taking backups, or where a number of different commands are used, to create backups, the label should also include the commands used, to create the backup.

Most backup media are sensitive to heat, humidity, direct sunlight and dust. So, it is imperative that they be stored in a cool, dry place. Ideally, media should be stored in an environment, with the temperature between of 62 to 75 degrees Fahrenheit, at a 40 per cent humidity level. Keeping backups in the same room as the system, may be convenient, but is not advocated. If such a room is struck by disaster, the backup media could also be destroyed.

Retrieval

- Backups should be tested for irretrievability/recoverability of information.
- Testing should be done on a test bed.
- Testing should never be tried in a 'live' area, for it could result in loss of live data.

BACKUP PROCEDURES

Daily Backup

- The daily backup should be taken, for all the databases, and other work areas.
- The daily tapes should be labelled, properly for this purpose.
- This backup should have two copies, with one copy stored in the production (say, data centre) and the other, in a safe and secure, off-site location.
- The daily tapes may be reused, at the start of the subsequent week. An example is given below.

Weekly Backup

- The weekly backup should be an aggregation of the daily backups.
- Backup for each week, should be taken on a separate tape.

- This backup should have two copies, with one copy stored in the production and the other, in a safe and secure, off-site location.
- The tapes used in this backup, may be reused after 1 month, i.e. after the monthly backup, has been taken.

Example

- Daily backups are taken, on all the seven days of the week, with the cycle starting from, Monday to Sunday.
- There should be seven tapes labelled, for each day of the week.

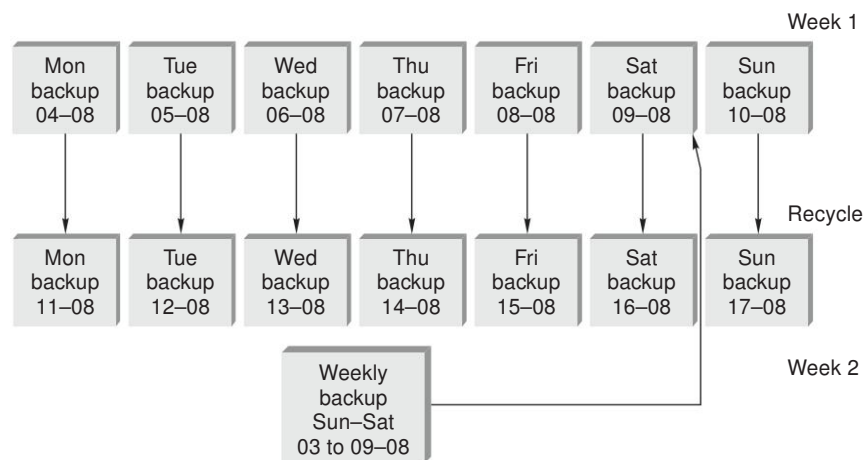


Fig. 9.2 Sample backup schedule

- Suppose the weekly backup is taken on Saturday 09-08-2003, then this weekly backup will contain all the backup, starting from Sunday (03-08-2003) to Saturday (09-08-2003).
- On the subsequent Monday (11-08-2003), for daily backup, use the tape, labelled 'Monday'. This tape was previously used, on Monday (04-08-2003). The data for this date (04-08-2003) is already available, on the weekly backup tape (03 to 09-08-2003).
- Continuing this way, on Saturday, daily backup and weekly backup is taken.
- Hence, the tapes can also be recycled and used effectively and efficiently.

Monthly Backup

- The monthly backup should be taken on separate tapes, for each month.

- The backup should be taken, for all the databases, operating system, application, system state and software.
- This backup should have two copies, with one copy stored in the production and the other, in a safe and secure, off-site location.
- The monthly tapes may be recycled after the end of each quarter, i.e. after the quarterly backup has been taken.

Quarterly Backup

- This backup should be taken, similar to the monthly backup.
- The monthly backup should be taken on separate tapes, for each quarter.
- This backup should have two copies, with one copy stored in the production and the other, in a safe and secure, off-site location.
- The monthly tapes may be recycled, after the end of each year, i.e. after the annual backup has been taken.

Annual Backup

- The annual backup should be taken at the end of each year.
- This backup should be a total backup, that includes all the application software, databases, system state, operating system and all profiles.
- This backup should have two copies, with one copy stored in the production and the other, in a safe and secure, off-site location.

Archive for Annual Backup

At any time, the production (DC) should have a copy of the weekly, monthly and quarterly backups. Since these backup media are recycled, they need not be archived. Only the annual backups should be archived, at the controlling office or in an off-site location, on the completion of a certain number of specified years, say, the fourth year.

- At any time, the DC should have backups of the previous three years.
- For example, at the start of the year 2004, the annual backup copy of the year 2000, may be sent to the Head Office, for permanent archival.
- The copy of the backup, in the off-site location, may be preserved there, itself.

BACKUP TECHNIQUES

The backup technique to be employed in an organization, is dependant on the media and the file structure. Accordingly, the various backup techniques, used in the organizations, are as follows.

Grandparent-Parent-Child (GPC) Backup

This technique is used in the case of sequential file batch system. In this case, the backup procedure begins, when the current master file (the parent), is processed against the transaction file, to produce a new updated master (child). With the next batch of transaction, the child becomes the parent (current master file) and the parent becomes the backup (grand parent). The new master file that is updated, becomes the child. This procedure continues, with each new batch of transactions, creating a series or generations of backup files. When the desired number of backup copies is reached, the oldest backup is erased. In this case, if the current master file is deleted, then the same can be processed from the current transaction file.

In such kind of techniques, the number of backup files needed for each application, is dependant on two factors, viz. one, the relative sensitivity/ importance of the application to the organization and second, the degree of file activity, i.e. number of times the master file gets updated.

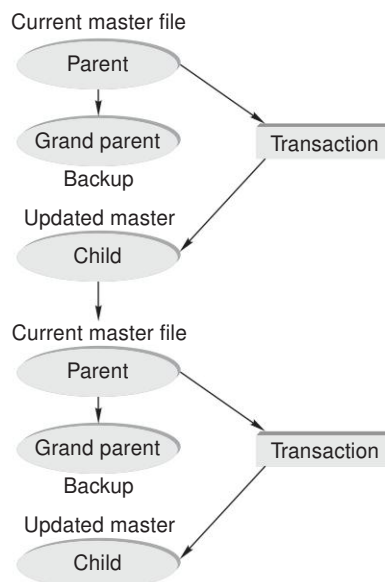


Fig. 9.3 GPC technique of backup

In case of auditing the GPC techniques, the auditor should select appropriate samples of systems and determine, from the system documentation, if the number of GPC backup files, specified for each system, is adequate, so that in case of contingencies, data loss will be minimal.

Direct Access File Backup

In case of direct access file backup techniques, once the data value is changed in the file, the original value is destroyed, leaving only one version, i.e. the current version. Therefore, to provide backup, the files must be copied, before being updated. This process of updation of the master file, is called destructive replacement.

The timing of the direct access techniques, will again, differ in a batch processing system and in a real time system. In case of a batch processing system, the backup is planned before the updating of the master file, whereas in case of an online or real time system, since transactions are processed continuously, the backup procedure takes place, at specified time intervals throughout the day. This time window is again, dependant on the sensitivity of the data files, to the organization.

Auditing direct access backup, needs, observation of the process, verification of the documentation, to find out if in case of batch updating, the data files are copied before updation and in case of real-time system, a proper time window is maintained, as per the sensitivity of the data and organizational requirements.

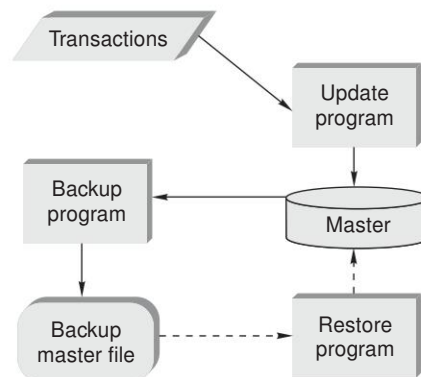


Fig. 9.4 Direct access file backup in a real-time processing system

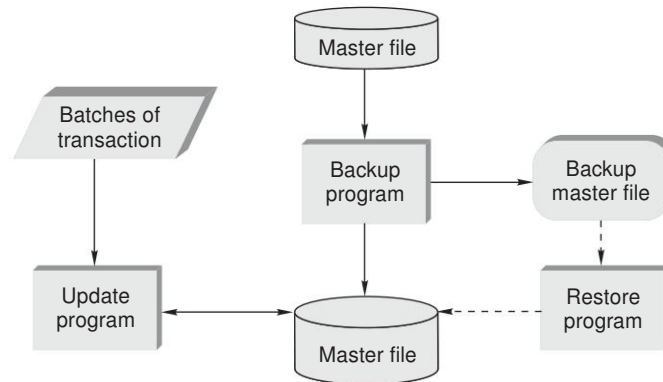


Fig. 9.5 Direct access file backup in a batch processing application

BACKUP CONTROL IN THE DATABASE ENVIRONMENT

One of the innumerable tasks of the DBA, is to ensure that all the databases of the enterprise, are always "available." Availability in this context means, that the users must be able to access the data, stored in the databases, and that the contents of the databases must be current, consistent and correct. It must never appear to a user, that the system has lost the data or that the data is inconsistent. This would totally ruin the user's confidence, in the database, and in the entire system.

Many factors threaten the availability of the databases. These include, natural disasters such as, floods and earthquakes, hardware failures, for example, a power failure or disk crash, software failures such as, DBMS malfunctions (read "bugs") and application program errors, and human failure, for example, operator errors, user misunderstandings, and keyboard trouble.

In a large enterprise, the DBA must ensure, the availability of several databases, such as the development databases, the databases used for unit and acceptance testing, the operational online production databases (some of which may be replicated or distributed, all over the world), the data warehouse databases, the data marts and all the other departmental databases. All of these databases, usually, have different requirements for availability. The online production databases, typically, must be available, up-to-date and consistent for 24 hours a day, seven days a week, with minimal downtime. The warehouse databases must be available and up-to-date, during business hours and even for awhile, after business hours. On the other hand, the test databases need to be available, only for testing cycles, but during these periods, the testing staff may have extensive requirements, for the availability of their test databases.

For example, the DBA may have to restore the test databases to a consistent state, after each test. The developers often have, even more adhoc requirements, for the availability of the development databases, specifically towards the end of a crucial deadline.

With such varied requirements, it will not be possible for the DBA to use different techniques, in taking the backup. Therefore, most Database Management Systems (DBMS), have inbuilt utilities, to take backup, both, logical and physical. Logical backups are used to take a "picture", of the data and structures, within a database, at a specific point in time. Logical backups export all data and structure definitions, from the database via, the export utility. They can contain structure definitions of tables, indexes, sequences, procedures, and so on, as well as, table data. They can cover the full database or only part of it, for example, specific tables or objects, belonging to specific schemas. The output of this utility, is a proprietary format, often called an "export" or "dump" file. Logical backups are restored, by recreating all, or part of a database, from ground-up via, the "import" utility. They are used frequently, in development environments or while moving data, from one database to another.

Logical backups are not considered as production grade, because they do not provide full recovery, in the event of a system crash. Recovery from a logical backup, after a system crash, would be devoid of all transactions, occurring between the time of export and the crash, itself and the database would be recovered, only upto the point in time, when the backup was taken. They are, however, often used for development and test environments.

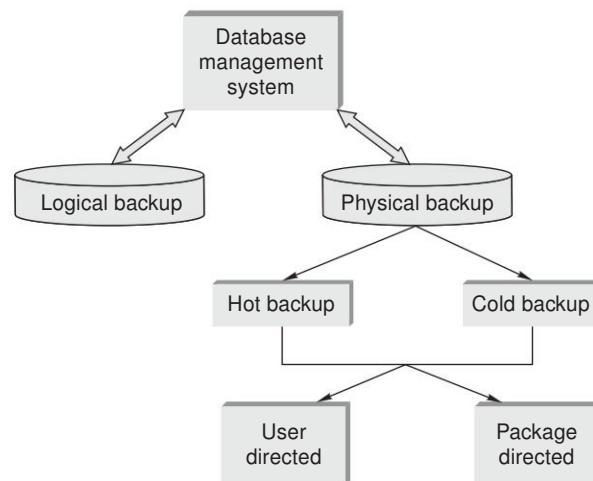


Fig. 9.6 Backup in database management system

Physical backups are copies, of the underlying physical volumes and files, that make up a database. Physical backups can be broadly classified into two viz. cold backup and hot backup. “Cold” backups are those, that occur, while the instance is down. “Hot” backups occur, when the instance is up and the database is available. All these backups can be either, “user-directed”, i.e. managed by scripts or programs that have been developed in-house, or “package-directed”, i.e. managed by a purchased, storage-management package.

MANAGEMENT OF IS OPERATION

The success of IS operation, depends on the appropriate resources, available to the operating professional and it is the IS management that is responsible, for providing the necessary resources. Apart from resource allocation, the IS management is also responsible, for establishing the necessary standards and procedures, or establishing all operations, in accordance with the overall business strategies and policies. Management feedback is essential for effective functioning of IS operation. The various management controls that are necessary for the IS operations are:

- Ensuring that there are appropriate policies and procedures for IS operation,
- Ensuring that there is segregation of duties and staff rotation, among IS operating professionals,

Box 9.1

Three fundamental objectives of segregation of duties

- Segregate the task of transaction authorization, from transaction processing,
 - Segregate record-keeping, from asset custody,
 - Divide transaction processing tasks, among individuals so that the perpetration of a fraud, will require collusion between, two or more individuals.
-
- Monitoring operations, to ensure compliance with set standards,
 - Reviewing operator log, to identify variances, between scheduled and actual activity,
 - Reviewing console log activities, during system shut down and hardware/software reinitialization,

- Monitoring system performance and resource usage, to optimize computer resource utilization,
- Ensuring that performance requirements, are included in all the IT development/acquisition and maintenance projects,
- Critical infrastructural components are to be identified and continuously monitored,
- Anticipating equipment replacement/capacity to maximize, current job throughput, and to strategically, plan for future acquisitions,
- Ensuring continuous services to the users,
- Maintaining job accounting and audit reports.

The IS operation management, should ensure that it gets a comprehensive report on the health of the important IS equipment, so as to initiate appropriate preventive measures. A sample, weekly server report, having different parameters for the activities and health of the server, is produced in Table 9.2.

Scheduling is a major function, within the IS department and it seeks to ensure that:

- Computers are used for authorized purposes,
- Consumption of system resources is efficient,
- The conflicting demand on the resources is minimized.

The IS operation management should ensure that, a schedule is prepared, based on the processing requirement and business priority and is implemented by the operation team. While preparing the schedule, it should be ensured that high-priority jobs are provided with optimal resource availability, while maintenance functions, such as, backup, etc. should, if possible, be performed during non-peak hours. For example, in case of a service branch of a bank, the maximum pressure, is at the time of various types of clearing activity. During such time, there is a need to generate statements, using network line printers. If other routine jobs, are also submitted to the printers, at the same time, it may delay the clearing process, which is very vital. Therefore, this call for, scheduling the print jobs and giving priority to jobs, related to clearing, during specific time periods. Similarly, there can be another case of bandwidth hungry applications in ATMs, like, uploading the Positive Balance File (PBF) to the ATM switch, by the respective non-Core Banking Solution branches (Non-CBS). Such activities, if done during the peak hours, will affect the normal transactions. So, this is an apt case of scheduling it to non-peak hours.

While some of the schedules, like, backup, temporal restrictions, etc. can be implemented at the system software level, most of the production schedules can be enforced, by the Automated Operation Facility (AOF). Where AOFs

Table 9.2 A sample, weekly server report

Weekly server report																
Server name	Date	Diskspace		Created				Deleted				Anti-virus status	Remarks	Back up date	Maintenance carried	Down time
		Utilized	Remaining	Users	Folders	E-Mail	Alias	Users	Folders	E-Mail	Alias					
Server-1	28/5/04	35.25	100.4	0	0	0	0	0	0	0	0	Up-to-date				
Server-2	28/5/04	48.61	100.4	0	0	0	0	0	0	0	0	Up-to-date	Details taken from server, on 28-05-04 Time: 4:50 pm Twice restarted. DLT drive was replaced.	28/5/04	DLT drive replaced.	15 mins
Server-3	28/5/04	25.95	109.7	0	0	0	0	0	0	0	0	Up-to-date				
Server-4	28/5/04	85.24	714.03	0	0	0	0	0	0	0	0	Up-to-date		28/5/04		
Server-5	28/5/04	9.62	24.26	0	0	0	0	0	0	0	0	Up-to-date				

are not used, the operation managers must monitor, compliance with the production schedule. Even in case of AOF, the operation management should periodically, review the operator log, to identify variances, between scheduled and actual activity.

From an audit perspective, the auditors should check the existence and enforcement of a production schedule, and verify various operating logs to ensure that the schedules are adhered to. In case of AOFs, there is also a need for checking the logs and the parameters of the AOF, to ensure that no unauthorized change is made to the AOF parameters and to the related non-scheduled activities.

Auditors also have a reason for concern, in the absence of any schedule. In such cases, auditors should first, analyse the need for a schedule and if there is a case for the need for a schedule, then in the absence of the same, auditors should expand substantive testing, to determine if unauthorized activities are being performed, using the IS resources.

CONTROLLING THE INPUT/OUTPUT (IO) FUNCTION

Input/output control, in an IS operation, has tremendous relevance in a batch processing system. In such cases, IO control personnel are responsible, for ensuring that batch processing information, is processed accurately and completely, in accordance with the intent of the IS management and its authorization. In case of online data processing, the input and output functions are carried out by the individual, and most of the controls are taken care of, at the application stage. But, there are certain application systems, where the output from one system, becomes the input for the next system. While individual applications are maintained online, files are transferred between the applications, using a batch file transfer mechanism. Such a mechanism is controlled by the job scheduler. The access to the job scheduler is very important, as any change in the job schedule, will not make available, the input files, to the successor applications, causing the production process, to halt.

The various operation controls that have to be exercised by the input/output group of IS operation areas are given below:

- Inputs are processed, accurately and in a timely manner,
- Output is produced in a proper format and distributed to the appropriate personnel,
- Reconciliation of hash total, in case of batch input,
- Data integrity is maintained, till it is accepted by the application system.

AUDITING THE INPUT/OUTPUT OPERATION

The audit procedures for reviewing the input/output control are as below:

- Verifying the policies and procedures and ensuring that IS personnel are adhering to established policies,
- Ensuring that proper segregation of duties is maintained,
- Verifying the various control reports and ensuring that these are accurate and complete and are made available to the IS operation management, as and when required,
- Ensuring that the authorization form, from the user department, is complete and has been appropriately authenticated,
- Program change control,
- Librarian function,
- Procedures for monitoring, efficient and effective use of resources.

DOCUMENTATION AND PROGRAM LIBRARY

Documentation, helps the operational group of the Information System area, in two ways. First, it serves as, a preventive control for asset safeguarding and data integrity, of the IS and second, as a tool for the operation management, to fix responsibility, on the appropriate personnel, in case of any eventualities. The various types of documents, a typical IS operation group should have, and the salient features of some of the important documents, are discussed below:

System Administration Manual

The system administration manual, serves the purpose of, a sort of handbook for the system administrator. It should contain the following information:

- A brief description of the hardware and the system software, in the organization,
- The organizational setup of the IS operation,
- The roles and responsibilities of various functionaries, in the operation group,
- The domain security policy,
- Desktop policy,
- Antivirus updating policy,
- Patch updating policy,
- IP addressing policy,

- Relations with third-party vendors: roles and responsibilities of third-party vendors,
- Backup and restore policy,
- Change management policy,
- Maintenance/call logging policy,
- Emergency procedures,
- Reporting procedures (daily, weekly, monthly, etc.).

As the system administration documents, contain information, which can be used by a perpetrator to penetrate into the system, these documents should be marked 'confidential' and should only be used by the officials concerned.

Database Administration Manual

Like the system administration manual, the database administration manual also, serves as a handbook for the database administrator. Some of the important information that should be contained in the database administration manual, is as follows:

- Database user/group access policy, which describes, who provides database access, and the procedures for granting such access,
- Adding/ deleting users to from database policy, which mentions the person, responsible for adding and deleting users to and from the database. It should also contain, the procedures for adding/ deleting users,
- Setting user permissions for database policy: provide details of the person responsible for setting the permissions for users, on the database,
- Re-indexing database: provide the procedures and information on the person, responsible for re-indexing the database, after changes have been made,
- Packing/ compressing database: provide procedures and information on the person, responsible for packing/ compressing the database,
- Data entry/ modification/ deletion: provide details of the person(s) who are authorized to make changes to the database. Include, procedures for data entry, modifying, and deleting information from the database,
- Database reporting: Provide details of the person(s), responsible for database reporting. Include, the reports that are generated, time frames, due dates and storage of the reports,

- Database backup and restoration: provide the details of the person(s), responsible for performing database backup. This information should also be included in the contingency plan. Include, procedures to follow, if the database needs to be restored.

Inventory Register

Inventory of the entire hardware and software is very important, from an asset-safeguarding perspective. IS operation management has the responsibility, to maintain the inventory details. Some of the controls that are necessary for inventory management, are as follows:

- In case of hardware, like, servers, PCs, Printers, etc. as far as possible, the inventory register, should be an output, of the inventory management application.
- In case of absence of any software application, for inventory management, the operation management should have, a proper process for hardware acquisition in place, and the entry in the register should be made, as soon as the materials are acquired.
- Once the hardware is acquired, it may be necessary to move it from one place to another. The organization should have policies for dealing with such movements, so that reconciliation of dead stocks, become easier.
- The inventory register should have the following particulars:
 - Date of acquisition,
 - Cost of acquisition,
 - Supplier,
 - Warranty,
 - AMC status,
 - Identification details,
 - Transferee location and code,
 - Location installed, and
 - Asset owner.

In case of software, the Information System operation, has the responsibility of managing the organization's inventory of acquired software or license software, apart from maintaining the inventory register. If this inventory software is not maintained properly, several problems will crop up, namely, (1) too many copies of the software, which are not required by the organization may be produced, (2) Illegal copying of the software, (3) use of software,

Table 9.3 A typical format of an IT register[illegible]

contrary to the terms and conditions of the licensing agreement, etc. Such problems can be mitigated, if the IS operation, takes the responsibility for, maintaining records, purchasing and using of software and its associated documents, and for ensuring that users comply, with the terms and conditions of the licensing agreement.

There are automated software available, which can be used by the operational group, for tracking and monitoring the assets, in the computer. These assets include, the software, hardware components, etc. Although these automated software are fairly effective, the IS operation management should impose certain restrictions on the end-users, to prevent them from disabling the software, from their system of start-up configuration. The users should not be given administrative access privilege. There are also some software metering packages, which will produce a report, of the use of various software vis-à-vis the license software.

Table 9.4 A typical format of a software license register

Owner: <name and designation of the owner of the register>					
Application:			Application owner:		
License type	License number	Acquisition date	Number of licenses	Cost	Comments

Apart from maintaining all the above documents, the IS Operation should also maintain, ancillary documents, namely, operational manuals, user manuals, vendor-supplied documents, books, and journals, etc. Although most of these documents are now, kept in an automated form, using various document management systems, the hardcopy documents still have several advantages, over the online documents. Some of the advantages of hardcopy documentation are as follows:

- Authentication in the hardcopy is easier to manage, than in the case of online documentation,
- Storing and retrieving, is easier in a hardcopy document,

- Hardcopy documents, can easily be produced as evidence, whereas, in case of online documentation, only the law of the country can allow/ disallow these, to be produced as evidence.
- The IS operation has the responsibility for managing the documents and programming library, which support their functions. The various responsibilities of the IS operation in this regard, inter alia, include:
 - Ensuring that proper documents exist, for various operational activities,
 - Ensuring that these documents are stored securely,
 - Ensuring that there is no unauthorized access, to the content of these documents,
 - Ensuring that sufficient backup exists, for documentation.
- In big IS installations, sometimes it is necessary to have an exclusive functionary, namely, documentation librarian, whose responsibility is, to manage the various documents, supported on user computers and the Local Area Network. When documentation is maintained on magnetic media, then the librarian has to, liaise with the security administration and database administration, to ensure that adequate access controls, are in place, and working effectively, to restrict access to documentation, only to authorized persons.

AUDIT OBJECTIVE

In case of, auditing documentation and programming library function of an Information System, the auditor can use interviews, observations and the review of various documents, to evaluate the following:

- Whether documents exist for frequent and also infrequent operational activities,
- Whether these documents have been authenticated by the appropriate authority,
- Whether there is a proper change management procedure, to update the various documents,
- Whether the processes followed, are as per the documents,
- Whether the processes entailed in the document, are as per the contemporary and international standards,
- If the documents are in electronic format, what are the accesses controls, applicable to these documents? And whether there are backup copies of these documents, kept in a secure location,

- Whether the physical balance of the inventories, tally with the balances in the register,
- Whether the software usage, is as per the existing licenses.

CONTROL OVER CONSUMABLES

Production or functional people, mostly use, computer consumables. Of course, the IS operational group also uses consumables, for its own use. Now, the question that arises is, who should be in charge of acquiring and distributing the computer consumables? Should it be, the operational group or the functional group? In case the operational group is assigned this job, then it has to perform all allied activities, related to acquiring and distributing the consumables, which are not core activities of the computer operation. Therefore, as per the industry practice, the work of acquiring and distributing the computer consumables, is always entrusted to the functional group. While the production group should ensure that adequate stock of consumables, are available for use, the IS operation group should give necessary information to the production group, about the specifications of the consumables and the requirements, from time to time. The IS operation group, also has the responsibility, to spread awareness, about the secure use, of computer consumables.

MAINTENANCE AND CONTROL, RELATED TO REMOVABLE STORAGE MEDIA

Removable storage media, are the alternative or parallel sources of secondary information storage, of the organization. So, they should have the same kind of controls as those of the usual, secondary storage devices, like, hard disks, attached to the computer. Otherwise, there are possibilities, of loss of data integrity. In fact, removable storage should have some additional controls, than those available in the case of hard disks, because:

- The removable storage is outside the controls, implemented through the operating system,
- These, change hands more frequently, than in the case of primary storage,
- Increasing order of read and write errors, in the removable storage, as compared fixed storage.

Now, let us discuss, the various controls that are necessary for removable storage media.

SELECTION OF STORAGE MEDIA

Any physical storage medium is, by definition, completely dependent on specific combinations of hardware and software, for access. The accessibility of information, stored on such media is therefore, highly vulnerable, in today's rapidly evolving technological environment. This issue is not solely, the concern of digital archivists, but of all those, responsible for managing and sustaining access, to electronic records/ data, over relatively short, even timescales.

Technological obsolescence, in removable storage media, is inescapable, irrespective of its physical longevity. So, there is a need to periodically refresh, electronic records, onto new media, depending on the contemporary technology. Nevertheless, careful selection of appropriate media, can maximize the periods between refreshment cycles and also simplify the refreshment process, in addition to providing the most secure storage environment, possible.

The following criteria should be considered, by IS operational management, when selecting removable storage media:

- Longevity
- Capacity
- Reusability
- Viability
- Obsolescence
- Cost
- Susceptibility

These criteria are elaborated here.

Longevity

For sensitive and long-term storage requirement, the media should have a proven life span of at least 10 years. Greater longevity however, is not necessarily an advantage, since obsolescence of drive technology, usually precedes, physical deterioration of the storage medium.

Capacity

The media should provide a storage capacity, appropriate for the quantity of data to be stored, and the physical size of the storage facilities, available. Minimizing the number of actual media to be managed, will usually, create efficiency and resource-saving.

Reusability

The media should have the facility, to be reused after short storage intervals (weekly, monthly, etc.). This allows for effective utilization and storage of the media, while at the same time, being cost effective to the organization.

Viability

The media and drives should support, robust error-detection methods, for both, reading and writing data. Provision for testing the integrity of media after writing, is also a benefit. Proven data recovery techniques should also be available, in case of data loss. Media should be write-once, or must have a reliable write-protect mechanism, to prevent accidental deletion and to maintain the evidential integrity of the data.

Obsolescence

The media and its supporting hardware and software, should preferably, be based on mature, rather than leading-edge technology, and should be well-established in the market place and should also be widely available. Media technologies, which are based on open standards for both, media and drives, should generally, be preferred to those which are of a proprietary nature.

Cost

Two elements, must be considered, when assessing the relative costs of storage media, viz. the 'cost of the media' and the 'total cost of ownership'. Valid comparisons of media costs, must always be made, on a price per MB/GB basis. The total cost of ownership will include, costs for purchasing and maintaining the necessary hardware and software, and of any storage equipment required. Support costs and the quoted Mean Time Before Failure (MTBF) of the relevant drive, must also be taken into account.

Susceptibility

The media should have low susceptibility to physical damage, and should also be tolerant to, a wide range of environmental conditions, without data loss. Magnetic media should have a high coercivity value (preferably, in excess of 1000 oersteds), to minimize the chances of accidental erasure. Any measures, required to counter known susceptibilities such as, packaging or storage requirements, should be affordable and achievable.

In situations where, multiple copies of data are stored on separate media, it may be advantageous to use different media types for each copy, preferably, using different base technologies, for example, magnetic and optical. This reduces the overall, technology-dependence of the stored data. Where the same type of media is used for multiple copies, different brands or batches should be used in each case, to minimize the risks of data loss, due to problems, with specific manufacturers or batches.

Coercivity is a measure of the amount of magnetic field required, to reduce magnetic induction to zero, i.e. erase the medium.

Oersteds are the unit of measurement for magnetic field intensity.

Location Control of Storage Media

Location or storage of removable storage media, is as important as the location of other important IS equipments, like, servers, etc. As these storage media are a secondary source of data, they should have the same kind of environmental controls, as the primary data-store, but at the same time, it should be ensured that both, primary and secondary data-stores, are exposed to the same kind of vulnerabilities. Even in the case of onsite locations, the removable media should not be kept in the same server room. It should be kept, preferably, in the adjacent room and access to that room, should be restricted. If possible, it should be placed under the control of the tape librarian. Both, onsite and offsite facilities, should maintain constant temperature and dust-free environment, to reduce the likelihood of damage to the media. In no case, should the removable media be kept, in unlocked drawers or cabinets.

To manage backup and restoration, of a large Information System area, there is a need to automate the operations by the use of an automated tape library system. Such an automated library system, typically, records the following particulars:

- Identifier for each storage medium
- Location identity of the storage medium
- Name of the operator who has the ultimate responsibility for a particular storage medium
- File, stored on each medium
- Authorized persons to access the storage medium
- Date of purchase of the medium
- Access history of the medium
- History of the read and write errors

- The age of the data and retention date
- Date when the medium can be released from the library
- Date on which the storage medium was last returned to the file library.

The automated tape library is a sort of AOF (Automated Operation Facility). So, the controls related to AOF, as discussed earlier, will be applicable to this.

Usage of Removable Storage Media

Sometimes the business requirements for storage media, require these, to change hands, frequently. For example, people requiring old data, will require the media, containing that data from the tape librarian, or personnel at the offsite location, will receive media from the production site, for storage, etc. In all these cases, there should be necessary controls, to ensure that the confidentiality, integrity and availability of data, are not compromised. The various controls, required for usage of removable media, are as follows:

- All users of the information, should be made responsible, for securely storing and disposing any storage media, which is used by them and is under their control
- All the removable electronic storage media, i.e. floppies, Zip tapes, etc. should be removed from each PC and properly stored, in a locked drawer, at the end of the workday
- All floppy disks and compact disks, should be kept inside a protective cover
- All floppies and compact disks should be properly labelled
- Users should ensure that all floppies and compact disks are kept away from hazardous substances, such as, moisture, heat, dust, magnets, etc.
- Users should be instructed to reformat or delete the data on the magnetic media, before disposing off the media
- As far as possible, the tape managements, system should be automated
- There should be proper change management procedures, for handing over the media to a third-party
- Maintenance and disposal of storage media

The reliability of the storage media, is a function of, proper usage and the age of the media. While proper usage can be implemented through policies and procedures, the deterioration in reliability because of age, should be

monitored. Records of the difficulties, experienced with storage media should be maintained. In fact, some software package, can be used to monitor the health of the media, which will enable a periodic preparation of reports for the IS operation management, to help them, take preventive action. Storage media like, tapes, should not be kept unused, for a long time because, over a period of time, pressure builds up in the centre of the tape, on its hub. This pressure, is caused due to bonding and compression of the materials, from which the tape was made. As a result, the tape can become unreadable. If there exists, a business requirement, to save the backup for long periods, then, the backup tapes, at periodic intervals, should be rewritten onto another media, to prevent the occurrence of the read/write error, due to the age factor.

When the storage media becomes unreliable, the best way to deal with the problem, is to discard it. But before discarding it, one must ensure that all the sensitive data has been removed from the media. Such objectives however, cannot be achieved, by simply deleting the files. Deleting the files, alters only the header information, which only makes the file unreadable, while the data, remains intact. Even bulk erasers, will leave traces of the data, on the media. So, the only way to discard the media, possessing sensitive data, is to perform a complete sanitization of data, before discarding the media. *Sanitization* is 'the process by which, data is removed, from Information Technology equipment and storage media, and rendered unrecoverable'. It includes, overwriting, degaussing and physical destruction. *Degaussing* is 'a process where, the magnetic media is exposed to a powerful alternating magnetic field'. This helps remove, previously written data, leaving the media, in a magnetically randomized (blank) state.

AUDIT OBJECTIVE

In case of auditing the removable media management of the organization, the auditors will conduct interviews, observe the process and verify the documentation, to assure the management that the sensitive data are securely backedup and that there is no loss of confidentiality and integrity of the data, backedup in the media and that asset safeguarding has been taken care of. Some of the steps which the auditors should take, to give an opinion on this, are as follows:

- Engage in a discussion with the onsite and offsite librarian, to determine the procedures that they follow, before they issue the storage media, to others,
- If log, of the storage media use, is maintained, then, the auditor can review the log and find out, if there has been any unauthorized access,

- If, by chance, the auditor finds any removable storage media, lying around, unattended, then he/she should try to find out, if such media contains any sensitive data,
- The auditor should also verify the procedures, for media handling, disposal, etc. to ensure that these are, as per the industry standards and take into account, the security requirements of the organization.

TECHNICAL SUPPORT AND HELP DESK

One of the important support functions of the IS operation, is to provide technical support and help desk facilities to the end-users. The purpose of technical support, is to provide specialized knowledge to the production system and to assist in problem-resolution. Whether the help desk function, is directly carried out by the internal IS operation professionals, or it is outsourced to a third-party, depends on the nature of the organization, the size and complexities of the IS, and the importance of the IS, to the organization. The more the complexities and the greater the dependence on IT, the stronger will be the case, for outsourcing the help desk function, because of the following reasons:

- The outsource vendor will be able to give focussed attention to the outsourced facility,
- Monitoring the outsource vendor, will be easier,
- Outsource vendors will process, be relatively better skills due to the varied exposure they receive,
- Economy of scale, due to reuse of components and skills, by the outsource vendors,
- The organization will be relieved of performing, routine activities of technical support and help desk facilities and consequently, concentrate will be able to on its core activities.

Whatever be the business model, i.e. outsourced or in-house, the IS operation management, has the ultimate responsibility, to ensure that there is no disruption in the Information System function, which may affect the business adversely.

Some of the characteristic functions of the help desk/technical support area, are as below:

- Attending to the queries of the line/functional departments/areas and resolving their problems, related to IS operation,
- Problem resolution can be undertaken both, onsite and offsite, depending on need,

- Training the end-user, on the proper and efficient use of the Information System,
- Acquisition of hardware and software, on behalf of the end-users,
- Controlling the installation, of vendor and system software, to improve its efficiency and to customize the system, based on organizational requirements and computer configuration,
- Documenting the problems and prioritizing them, as per need,
- Forwarding the unresolved problems, to the appropriate authority,
- Closing out the resolved problems, with proper documentation.

Help Desk Function and Knowledge Management

The IS operation professionals, in the help desk/ technical support area, should possess the following, to function, effectively and efficiently:

- Technical knowledge of diverse technologies,
- High level of inter-personal skills,
- Ability to react fast.

Organizations should develop the help management system in such a way, that it not only helps in logging the complaints/calls, but also helps the organizations, in providing necessary information, about the history of the Information System, which would help in taking decisions, regarding further Information System acquisition and plans, for necessary preventive maintenance. The flow of a help desk/ technical support function, is appended below:

Box 9.2

Logging the call made by the end-user, with the inventory number and name of the person, who logs the call



Displays the particulars of the Information System, viz. item name, date of purchase, name of the vendor from whom purchased, system configurations, warranty or Annual Maintenance Control (AMC), last problem resolved/unresolved, name of the engineer who last attended the call.



(Contd)

Assigns a call tracking number and the call gets forwarded to IS operation.



IS operation assigns problems to a particular engineer, with priorities set, if required.



Engineer logs in and sees the details of the problem, and the history of IS, and then, takes a decision, to solve the problem, either through onsite visits or offsite telephonic advise or by forwarding it to higher professionals.



If resolved, the problem is closed, by the engineer.



Unresolved problems, automatically get forwarded to appropriate operation management, after a specified period of time.

In the above kind of a structure, organizations not only, effectively, solve the problems in the IS, but also gather a lot of knowledge about the systems, and this knowledge can be used by them in future, to take management decisions with respect to Information Systems. For example, the following queries can be addressed, by the system:

- What are the most frequent problems in the hardware or software?
- What are the most frequent problems, which usually, take a long time to be resolved?
- What are the most frequent, unresolved problems?
- What are the areas/ departments from which, most of the complaints are lodged, during a specified time?
- Who are the vendors, whose products are giving frequent problems?
- Who are the vendors, whose products give the least amount of problems?
- Who are the engineers, who solve problems fast and efficiently?
- Who are the engineers, who take considerable time, to resolve problems?
- Who are the users, who logged most of the problems?
- How many problems are forwarded to higher-ups, during a specified time, etc.?

Such kind of information, if properly managed and analyzed, will give immense management-specific information, for the efficient and effective use, of Information System resources.

The Information System department itself, is a service organization, for the end-users and the success of this department, is dependant on, satisfying the processing and service requirements of the end-users. Many IS departments, define the minimum level of services, is guaranteed to the end-users. These levels of services are often documented, in the Service Level Agreements (SLAs). In case the services are outsourced and there is a contractual relationship with the outsourced vendor, the Service Level Agreement should address, the following five, key questions:

- What is the provider promising?
- How will the provider deliver on those promises?
- What are the key performance parameters?
- Who will measure delivery, and how?
- What happens if the provider fails to deliver, as promised?
- How will an SLA change over time?

At this stage, we will discuss, some of the key elements of the Service Level Agreement and also, the importance of Key Performance Indicators.

ELEMENTS OF SLA

- The SLA should have clearly- defined promises, made by the vendor. These promises, help to stay focused on customer requirements and are an assurance that the internal processes are following the right direction,
- The SLA should define the Key Performance Indicators like, response time, resolution time, turn around time, etc.
- Violations of the services, should be clearly defined. For example, the definition if 'violation', and the violation report and related penalties, should be calculated, preferably, on a monthly basis,
- User environment, viz. the architecture and technologies, used by the consumers of the services, should be mentioned in the SLA,
- The normal service availability and schedule availability, should be mentioned in the 'SLA events', that impact the services,
- The SLA can also include a wide range of financial performance measures, like, year-to-year cost reduction; human relationship measures like, resource planning, staff turnover, and also, development or training or risk management measures like, compliance with control objectives,

- Right to audit the third-party provider's facility, should be part of the SLA,
- If third-party service engineers are residents, in the customer's premises then, the necessary non-disclosure agreement and adherence to the relevant portion of the IS security policy, should be part of the SLA.

Importance of Key Performance Indicators (KPIs) in SLA

Key Performance Indicators are quantifiable measurements, that are agreed on, upfront, and that reflect the critical success factors, of an organization. They will differ, depending on the nature of the organization and the nature of the services. A business may have, as one of its Key Performance Indicators, the percentage of its income that comes from a particular business line or a group of business lines. A school's Key Performance Indicator, could be the graduation rates of its students. Likewise, in case of a SLA for the help desk/technical support, the KPI could be:

Response time, i.e. the interval between, the time, the user sends a request, to the time, the request is acknowledged by the engineer and expressed, in terms of, percentage of response time, more than 'X' seconds/minutes.

Resolution time, i.e. the interval between, the time the vendor/engineer acknowledges the request, till the time it is resolved and expressed, in terms of percentage of resolution, time, more than 'X' seconds/minutes/hours.

Turn around time, i.e. the interval between, from the time, the complaint/call is logged, to the time the call is resolved and measured, in terms of percentage of turn around time, more than 'X' seconds/minutes/hours, etc.

Whatever Key Performance Indicator is selected, it must reflect the organization's goals, must be the key to its success, and must also be quantifiable (measurable). Key Performance Indicators usually, are long-term considerations. The definition of what they are, and how they are measured, do not change frequently. The goals, for a particular Key Performance Indicator, may change as the organization's goals change, or as it comes closer to achieving a goal.

Management Control over SLA

Once the boundary is fixed and performance matrices are defined in the SLA, there is a need for the operation management, to have a close look at the performance of the operation and particularly, the unresolved problems, which

have been forwarded escalated, to them. Some of the tools that help the operation management in exercising such controls, are:

- Four blockers
- Fish bone analysis
- Root cause analysis
- Dashboards

Four Blockers

Hits	Misses
Plan of action	Strategy

Fig. 9.7 Four blockers

Four blockers is a management tool, where, for a particular time range, the management can view the number and nature, of calls/complaints, called *Hits*, which comprise the first block. The second block is composed of the action taken for these hits, called *plan of action*. The third block is that of *misses*, i.e. the unresolved problems and the fourth block indicates the *strategy*, for resolving the unresolved problems.

Fish Bone Analysis/Root Cause Analysis

Fish bone analysis, which is also called, *Ishikawa* analysis, named after Dr Kaoru Ishikawa, a Japanese quality control statistician, who invented the fish bone diagram, is an analysis tool, that provides a systematic way of looking at effects and the causes that create or contribute to these effects. Because of the function of the fish bone diagram, it may be referred to, as a cause-and-effect diagram. The design of the diagram, looks much like the skeleton of a fish and therefore, the name, fish bone.

Fish bone analysis is needed by the operation management, to study the details of unresolved problems and to determine their root causes, so as to make, the necessary quality improvements in the process.

How is a Fish Bone Diagram Constructed

- List the problem/issue to be studied, in the ‘head of the fish’,

- Label each "bone" of the "fish". The major categories, typically utilized are:
 - The 4 M's: Methods, machines, materials, manpower.
 - The 4 P's: Place, procedure, people, policies.
 - The 4 S's: Surroundings, suppliers, systems, skills.

Note: You may use any one of the four categories suggested, combine them in any fashion or make up your own combinations. These categories are to help you organize your ideas. You can:

- Use an idea-generating technique, e.g. brainstorming, to identify the factors within each category that may be affecting the problem/issue and/or the effect, being studied. The team should ask, "Why does this service of the computer, frequently hang?"
- Repeat this procedure, with each factor, under the category, to produce sub-factors. Continue asking, "Why is this happening?" and place additional segments under each factor and subsequently, under each sub-factor.
- Continue, until you no longer get useful information, when you ask, "Why is this happening?"

Analyze the results of the fish bone, after the team members agree that an adequate amount of detail has been gathered, under each major category. Do this, by looking for those items that appear in more than one category. These become the "most likely causes".

- For those items, identified as the "most likely causes", the team should reach a consensus, on listing those items in priority, order of with the first item, being the most probable" cause.

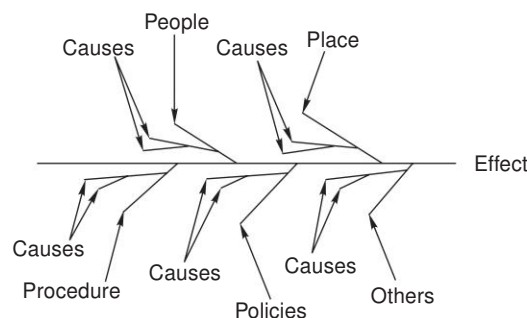


Fig. 9.8 Fish bone diagram

Dashboard

Dashboard helps the management, have a consolidated view of important issues. In case of help desk and technical support, the operation management can use the dashboard, to visualize the issues at the macro level, viz.:

- The top ten unresolved problems
- Ten frequently occurring problems
- Call/problems that persist beyond 72 hours, without resolution
- Analysis of the top contributor to the problem
- The asset, type and make, having frequent problems, etc.

The IS operation area is a service unit and as such, is always more of a cost center, than a profit centre. To make it a profit centre, the IT management sometimes, defines and uses billing and chargeback procedures, to encourage the proper use of computer resources and assure the user departments of fair treatment and of fulfillment of their needs. The rates charged, should reflect the associated costs of providing services.

AUDITING HELP DESK AND TECHNICAL SUPPORT

When performing an audit of this area, the IS auditor should first ensure, that adequate and documented procedures exist, to guide the IS operation personnel in logging, analyzing, resolving and forwarding the problems, in a timely manner, in accordance with the management's intent and approval. The following methods/procedures should be followed by the IS auditor, to be able to give an opinion on the subject area:

- Interview with the IS operation personnel, to evaluate their knowledge about policies and procedures, their level of satisfaction in the process and moreover, their competency in the area,
- Review the policies and procedures, to find their efficacy (remember that the policies and procedures, should have the management's approval),
- Review the downtime register, to find out the efficacy of the technical support function,
- Review the calls/complaints, which are booked during a certain specified time, to ascertain the following:
 - What is the average response, resolution and turnaround time?
 - Which are the frequently logged complaints and what has been the management's action, on those calls?

- Which complaints are simple enough, to be solved by the user himself/herself, with simple training/education or through some routine maintenance?
- What is the size of the unresolved problems?
- What are the material effects of the unresolved problems? For example, in case of a bank, how many times has the customer service been hampered, by the problem, etc.?
- What has been the management's action, on the forwarded calls?
- During the time of the review, observe the call logging process and the activities of the related personnel,
- Verify the chargeback procedures/algorithm, to understand, what costs are included in the chargeback.

In case the help desk function has been outsourced and resident engineers of the vendors, are posted in the premises, the auditor should in addition, follow the following methods/procedures:

- Evaluate the SLA, with the third-party, to ensure that the third-party providers' services, are properly identified and contracted,
- Interview the resident engineer, to ascertain his technical knowledge and knowledge of policies and procedures,
- Verify the educational qualifications of the engineers and ensure that these match the requirements, documented, in the agreement with the service provider,
- Verify if an appropriate non-disclosure agreement (that conforms to universal business standards, in accordance with legal and regulatory requirements, including liabilities) has been entered into, with third-party personnel.

Verify the minutes of steering committee meetings and other management forum meetings, to ensure that security issues, related to a third-party, are discussed in these meetings.

SOFTWARE MAINTENANCE

Software maintenance essentially envisages, maintenance of system software, viz. operating system, Database Management System (DBMS), etc. utility software and application software, both, outsourced and developed in-house. While the IS operational group has a direct responsibility for the maintenance of system software, the maintenance of application software (mostly the

outsourced one), is carried out by the respective vendor and is normally, governed by the maintenance contract, entered into, with the vendor. When we talk of maintenance of application software, what exactly do we mean by software maintenance, or what does it envisage? Does it mean debugging the software?, Loading of patches? Upgradation, of the software? Or, taking care of the wear and tear, in the application software? Or, is it a combination of all these?

If the application software, is developed taking the business logic into consideration and has been properly tested, then it should not have any logical error or bug. If at all any logical error occurs in future, then it means that there is a flaw in the software, which should be taken care of, by the software vendor, without any extra cost to the organization. As regards loading of patches and upgradation of software, if these are required by the organization, then of course, either there will be separate contract for these, or it will be a part of the maintenance contract entered into, with the vendor.

As regards wear and tear in the application software, there is a natural tendency of a system to move towards internal disorder and eventual collapse that is called 'entropy', in the case of software. This can happen in many ways. One form of internal disorder can occur, if there is a change in the business process because of the changes in the laws and regulations of the land. Consequently, the application system will become, less effective and efficient. An other form of entropy could be, the load factor, i.e. the number of transactions exceed the expected limit, which the application is unable to process. Another interesting form of entropy could be, gradual decline in the knowledge of the system, of the maintenance personnel. Entropy in an application system, can be controlled by, deploying concurrent auditing techniques and an appropriate preventive maintenance system, which will detect the entropy, at an early stage.

Therefore, the maintenance of the application software, is neither for debugging the software, nor for helping the users, operate the software. It is rather, taking care of the entropy or wear and tear. Now, let us discuss the control requirements for software maintenance.

- In case of the system software, the loading of patches that are released by the vendor, for known vulnerabilities, is a very important aspect of maintenance. Sometimes, the software will not be supported by the vendor, if the latest patches have not been updated. So, there should be a well-defined patch management policy, which should be strictly adhered to. Considering the large number of patches released by the vendors, it is sometimes difficult to keep track of all these patches and load these into all the enterprise systems, promptly.

Therefore, some organizations have a formal arrangement with the vendor that, as and when, there is any release of a patch, it should be pulled by in the organizations, automatically. In such cases, one system of the organization should be exposed to the Internet, so that it can download the patches, as and when released. After downloading the patches, these will be sent to all the enterprise systems, automatically. The control aspect, which is very important in such a kind of arrangement, is that, at the time of downloading patches from the Internet, the connectivity to the LAN should be blocked and at the time of uploading the patches to the LAN, the connectivity to the Internet should be blocked. In case connectivity to the Internet is through the LAN, the gateway security should be strictly enforced, during the "pull" mechanism (downloading patches from the Internet) and there should be no unnecessary traffic to the gateway, during the "push" mechanism (uploading patches to the LAN).

- When the patch is downloaded, the authenticity of the site, from which it is downloaded and the authenticity of the patch itself, are very important, from a control perspective. In such a case, the host level security, assumes a lot of importance.
- In case of application software, developed and maintained in-house, the most important aspect is, the maintenance of the source code and a formal process of change management. Any request for change to the software, should come from the user department and before the changed version or patch is loaded in the production system, it should pass from the test environment of the development team, to the staging environment (where there is exclusive testing) and finally to production. There should be a proper segregation of duties, among the testing, staging and production groups. This procedure of moving the program, from the testing, to the staging, to the production environment, is called turnover process.
- In case the application software is outsourced, the organization should have a structured, site-support, maintenance agreement with the vendor. Whenever there is a maintenance requirement, the call should be logged and a log book should be maintained, for entering the details of the calls logged with the vendor and the response time. This log should also mention, the type of problem in the software, so that this can be reviewed later on.
- The site-support, maintenance contract with the vendor, should inter alia, contain:

- A non-disclosure agreement, for not disclosing the data, which one would have access to, while maintaining the application,
 - Entry restrictions, as per access control security,
 - Entry restrictions to sensitive places like, data centre. In case of necessity, one official of the organization should accompany the vendor.
- In case the vendor wants to log into the system for maintenance, proper login authentication procedures, with requests and responses, should be followed.
 - Although the organization should have a policy for structured software maintenance, there should also be a policy for making emergency amendments, to software.

QUALITY ASSURANCE

Quality assurance in IS operation, is basically a preventive control, which ensures that the systems are authorized, tested and implemented in a controlled manner, before being introduced into the production environment. For example, in case of a banking organization, the quality assurance group will internally test all the applications, whether, developed in-house or outsourced, as per the parameters specified by the management, before it is rolled out.

The various objectives of the quality assurance functions, are as below:

- To ensure that the organization adheres to quality standards in IS operation,
- Testing the software, before it is put to use,
- Helping the organization, in evaluating large system projects, from the quality and control angle,
- Reporting to the management, about systems that are not performing as defined and designed.

Auditing the Quality Assurance Function

In case of auditing the quality assurance function of the IS operation, the auditor should give importance to the following aspects:

- There is sufficient segregation of duties, between quality assurance and other groups,

- The QA group, while recommending a quality standard, should take into consideration the relevant industry practices and international standards.

The QA professionals are appropriately trained, to discharge their duties.

PHYSICAL AND ENVIRONMENTAL SECURITY

All the environmental controls are aimed at minimizing the loss, resulting from naturally occurring events such as, fire, natural disaster (earthquake, volcano, hurricane, etc.), power failure, air-conditioning failure, electrical shock, equipment failure, water damage/flooding, bomb threat/attack. We will now discuss, some controls, to check such environmental exposures.

Physical Location

The physical location of the computer operation centre, directly affects the risk of disaster. To the extent possible, the computer centre should be away from human-made and natural hazards, such as, processing plants, gas and water mains, airports, high-crime areas, flood plains and geological faults. In case of multi-storeyed buildings, the computer operation should not be located in the basement, as this will be more vulnerable to flood and fire.

Construction

Ideally, a computer centre should be located in a single-story building, of solid construction, with controlled access. Utility (power and telephone) and communication lines should be located underground. The building windows should not be able to be opened. An air filtration system should be in place, that is capable of keeping out pollen, dust and dust mites.

Access

Access to the computer centre, should be limited to the operators and other employees, who work there. Programmers and analysts, who need access to correct program errors, should be required to sign in and sign out. The computer centre should maintain accurate records of all such events, to verify access control. The main entrance to the computer centre should be through a single door, though fire exits with alarms, are necessary. To achieve a higher level of security, access should be monitored by closed-circuit cameras and

video recording systems. Some of the first level security measures, which should be implemented at the entrance, are:

- Security guards should monitor movements of all persons, at the entrance,
- In case of termination of employment, security guards should be informed, of the last date of employment, of the terminated staff,
- All bonafide members of the organization, should be issued identity cards that establish his/her credentials. For larger locations, the identity cards may also have the capability to, control access to office locations, built into them,
- All employees should be ready to display their identification cards, at all times, inside the premises,
- Before allowing a visitor to enter, the security guard, should check with the person to be visited,
- Visitors should be given badges, which distinctly identify them as visitors, and these should be prominently displayed, while they are within the premises,
- Visitor's log will be maintained, at the entrance by the security guard and will be used to record the following details, about the visitor:
 - Name of the visitor,
 - Organization that the visitor represents,
 - Person the visitor intends to meet,
 - Purpose of visit,
 - Signature, and
 - Declarations regarding any laptops, storage media, etc. that the visitor may be carrying, inside the organization's premises.

Air-conditioning

Computers function best, in an air-conditioned environment. For mainframe computers, providing adequate air-conditioning is often a requirement of the vendor's warranty. Computers operate best, in a temperature range of 70 to 75 degrees Fahrenheit and a relative humidity of 50 per cent. Logical errors can occur in the computer hardware when temperatures depart significantly from this optimal range. Also, the risk of circuit damage due to static electricity increases when humidity drops. High humidity, on the other hand, can cause moulds to grow, paper products (such as source documents) to swell and equipment to jam.

Fire Suppression

The most common threat a firm's computer equipment faces, is from fire. Half of the companies that suffer fires, go out of business because of the loss of critical computer records. The implementation of an effective fire suppression system is therefore, much required for the organization. To suppress or extinguish the fire, we need to either, deprive the fire of oxygen/ fuel or lower the temperature. Fire suppressant systems normally, use a combination of both of these. These systems are a combination of both, detective and corrective control. They get automatically activated, immediately after the detection of high heat, generated by fire and consequently raise an alarm. It is vital for the alarm to be audible to the central security personnel. At the same time, other mechanisms in the system to localize the fire are triggered like, closing the fire doors, notifying the fire department (of the organization), closing the ventilation ducts and shutting down necessary electrical equipments. Although the medium used for fire suppression varies, depending on the need of the organization, it is usually, one of the following:

- The sprinkler system, is the traditional water-based system which, in case of a fire, automatically starts to sprinkle water over the fire. This kind of a system may deploy a dry pipe, attached to a pump. When a fire is detected, the pump gets activated and the pipe becomes charged with water for sprinkling. Such a system is good, in the sense that any leakage in the pipe will not result into leaking of water, but at the same time, it suffers from a time lag problem, from the time of fire detection to the activation of sprinkling. In case of a charged pipe system, the pipes are always charged with water, so that whenever a fire is detected, the sprinkling of water will start promptly. In this case, any leak in the pipe will also cause water leakage, and the entire computer system will be exposed to water damage.
- There are systems which use inert gases like halon, to remove oxygen from the air. This does not damage the equipment, unlike the water-based system. Such a system however, has got serious disadvantages. For example, it affects the ozone layer. In fact, in the Montreal protocol of 1987, production of halon was banned w.e.f. January 1994.
- FM-200 is another type of fire suppressant, which is discharged as gas, onto the surface of the combusting material. Large amount of heat energy is absorbed from the surface of the burning material, thereby lowering its temperature below the ignition point. The gases

released in the process are not detrimental to the health of human beings. Such systems are now, widely used in the industry.

- There is another system which releases pressurized carbon dioxide (CO_2) gas, to replace the oxygen required for combustion. Such a system, although highly effective, suffers from the disadvantage of having a lethal effect on the human life. So, in case of an unmanned data centre (AOF), where there are no risks to human lives, such systems can be used for effective fire suppression. However, care should be taken, for in some countries, automatic emission of such gas is prohibited, as per the law.

Smoke Detectors

Smoke detectors should be installed below the ceiling tiles, throughout the IS operation facilities and also below the raised computer room floor. This is a kind of detective control which gives off an alarm when it detects smoke. This alarm should be audible to the fire department of the organization and also, in the central security area.

Fire Extinguisher

Fire extinguishers should be kept near the equipments, throughout the facility. Since ultimately, the employees have to operate these at the time of need, proper training should be given to the users for operation. They should also be tagged for inspection and inspected at least annually. The basic difference between an integrated fire suppression system and a fire extinguisher is that the latter can put, the fire out but cannot localize it, whereas the former can do both.

The smoke detectors and, fire extinguishers should supplement, not replace, fire suppression system in a large IS installation.

Power Supply

Commercially provided electrical power, presents several problems that can disrupt the computer centre operations, including, total power failures, brownouts, power fluctuations, and frequency variations. The equipment used, to control these problems includes, voltage regulators, surge protectors, generators, and batteries. The extent and configuration of control equipment needed, will depend on the firm's ability to withstand such disruptions and the power company's record for providing reliable service. This can be an

expensive control decision and requires extensive analysis and also, the advice of experts. There may be a need to immediately shut off power to the computer and peripheral devices in case of fire, water leakage, etc. In such cases, two emergency power-off switches should be provided, one, in the computer room and the other, outside the computer room. Such switches should also be protected, as operation of the switches in case of non-requirement, are likely to cause a disaster.

Another important aspect which should be considered for continuity of power supply, is the deployment of Uninterrupted Power Supply (UPS). The control aspects of the UPS are as follows:

- The UPS should be installed in a room/cabin, which should be kept under lock and key,
- The UPS should be installed in a separate cabin/room and not in the same cabin/room as the servers,
- The UPS room should not be very close to the server room. This will help prevent the spread of fire resulting from a short circuit in the UPS room to the server room, or vice versa,
- The UPS room/cabin should have an independent access and access to it should not be through the server room. This will help obviate the need for the UPS maintenance personnel to pass through the server room,
- The room should be spacious enough to house the UPS, batteries and also provide for space for the maintenance personnel to move around,
- The UPS and batteries should be provided with the recommended ambience, with special attention to temperature control, humidity, dust free environment, etc.,
- If the batteries are of lead acid type (e.g. tubular), the UPS room should have sufficient ventilation. An exhaust fan should also be provided, to facilitate better ventilation. Providing for the UPS room/cabin near a window, will facilitate such an arrangement,
- It must be ensured that the UPS is not switched off and that the power cord is properly secured to the equipment. It must be also made sure that the battery cords are properly connected,
- It must be ensured that no unauthorized person tampers with or changes the switch-settings on the UPS,
- Generally the batteries of the UPS take 8 to 12 hours to get fully-charged. If the local power supply is erratic or if there is no power

supply for at least 8 hours in a day, suitable arrangement for the provision of a generator should be made,

- No load other than computer load should be allowed to be connected on the power supply from the UPS, as it affects the quality of power supplied to the computers.

AUDIT OBJECTIVES

To evaluate the controls governing the operational aspect of the Information System Area, the auditor should verify that (1) physical and environmental security controls are adequate, to reasonably protect the organization from physical exposures, (2) operator documentations are adequate to deal with system failures, (3) the operators are aware of the policies and procedures of the organization.

For achieving these objectives, the auditors have to verify all the controls, by visiting the location, verifying the documents and observing the procedures. Some of the audit procedures for these are as below:

Test of Physical Construction

The auditor should determine if the computer centre is solidly built of fireproof material. There should be adequate drainage under the raised floor, to allow the water to flow away, in the event of water damage from a fire in an upper floor or from some other source. In addition, the auditor should evaluate the physical location of the computer centre. The facility should be located in an area that minimizes its exposure to fire, civil unrest and other hazards.

Test of Fire-Detection System

The auditor should establish that fire-detection and suppression equipment, both, manual and automatic, are in place and are tested regularly. The fire-detection system should be able to detect smoke, heat and combustible fumes. The adequacy of these devices can be determined, by reviewing official fire marshal records of tests that are stored at the computer centre.

Test of Access Control

The auditor must establish that routine access to the computer centre is restricted to authorized employees only. Details about visitor access (by programmers and others), such as, arrival and departure times, purpose and

frequency of access, can be obtained by reviewing the access log. To establish the veracity of this document, the auditor may covertly observe the process by which access is permitted.

Test of Backup Power Supply

The computer centre should perform periodic tests of the backup power supply, to ensure that it has sufficient capacity to run the computer system and air-conditioning. These are extremely important tests, and their results should be formally recorded. As an organization's computer function develops, its backup power needs are likely to grow, proportionally. Indeed, without such tests, an organization may remain unaware that it has outgrown its backup capacity, until it is too late.

COBIT AND OPERATIONAL CONTROL

Operational control in COBIT is addressed in all the thirteen processes, in the domain of delivery and support. These thirteen processes and the number of detailed control objectives under these processes, are as follows:

Table 9.5 Operational control in COBIT

<i>Domain index</i>	<i>Process</i>	<i>Number of detailed control objectives</i>
DS1	Define service levels	7
DS2	Manage third-party services	7
DS3	Manage performance and capacity	8
DS4	Ensure continuous service	10
DS5	Ensure system security	13
DS6	Identify and attribute costs	3
DS7	Educate and train users	3
DS8	Assist and advise customers	5
DS9	Manage the configuration	6
DS10	Manage problems and incidents	3
DS11	Manage data	25
DS12	Manage facilities	6
DS13	Manage operations	7

These processes and their detailed control objectives are not under the scope of our discussion. However, readers are advised to refer to the COBIT material for insight into the same.

OPERATIONAL RISK FROM A BANKING PERSPECTIVE

After having discussed the various operational risks, arising out of IT operations and their necessary controls, some questions may come to the minds of the readers, particularly, the banking community about whether these are the same operational risks, about which regulators all over the world are worried? Are the risks arising out of IT operations, all about operational risk? If how do we quantify such risks, so that we can provide for it in our balance sheet, as required by the regulators? The next section will clarify such doubts and give a brief explanation for quantifying such risks.

In recent years, bankers and financial professionals have recognized the crucial and growing importance of operational risk management, and the field is currently undergoing a surge of innovation and development. Developments in IT and E-Commerce, large-scale mergers and acquisitions and increased outsourcing, all suggest that operational risk exposures are substantial and steadily growing.

WHAT IS OPERATIONAL RISK MANAGEMENT (ORM)

Simply put, it is a logic-based, methodical approach to making calculated decisions on human, material and environmental factors, associated with any type of activity or operations that are in turn associated with the business of banking. However, as per the definition given by the Basel Committee, the committee of the Governor's of Regulatory Authority of the G-10 countries, the operational risk is '*the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events*'. This definition includes operations risk, IT risks and legal risks and risks related to human resources, business processes and events, outside the control of bankers.

WHY IS OPERATIONAL RISK MANAGEMENT IMPORTANT

As business activities become more complex, the number and types of risks increase. As a result, more emphasis is being placed on increasing the standard of risk management practices, in order to help protect business viability and shareholder value. Organizations now recognize that they have a responsibility, not only to their management, but also and perhaps more importantly, to

their employees, shareholders and the general public, and to the regulators (both local, as well as global), to correctly manage operational risks.

The ORM process allows systematic risk decision-making that manages risk, as part of the whole operation, reduces mishaps and improves the cost-benefit ratio, by lowering risks. The end result is that the organization is safer, our resources are conserved and our operational capability is optimized.

HOW TO PERFORM OPERATIONAL RISK MANAGEMENT

As we mentioned earlier, ORM is a logical and methodological approach. The following are the steps involved in the ORM process:

Identify the hazards: A hazard is simply, a condition that could cause loss. It can also be called 'cause to loss event'. Identification is done by focusing on what is at risk and listing potential hazards.

Assess the risks: Here, we examine each hazard and determine the exposure, severity and the mishap-probability, associated with our activity. After a hazard is analyzed, risks can be clearly identified. Now, prioritize the hazards into different levels of risk and work on the most problematic level, first.

Analyze risk control measures: Determine which risks can be eliminated, reduced or controlled, in some manner. If you have done the previous step correctly, you'll know which risk to concentrate on, first. *Risk control must change the risks, by impacting the exposure, severity or the probability of a mishap.* Controls usually have an associated cost, in terms of the investment of time or money. Prioritize these control measures, to get the maximum 'bang for your buck'.

Make control decisions: This step involves the following two actions:

- (a) Select the best possible risk controls,
- (b) Decide if these controls will assure, that the benefits will outweigh the costs.

This decision-making process should involve the right person who will make the right decision, at the right time, based on the right inputs. You must always opt for risk control, especially when total benefits outweigh total costs. Similarly, always reject risk control, especially when total costs outweigh total benefits.

Risk control implementation: While implementing of controls, the most important thing to remember is that the risk controls should be truly integrated with the plans, processes and operations, with which they are associated. Without integration, risk control will not be nearly as effective. For the controls

to be successful, the implementation must be clear to everyone, there must be accountability and the organizational leadership must provide its support.

Supervise and review: When risk controls are properly integrated, their supervision becomes just like any other leadership action. This is the prime reason for the emphasis on completely integration of the risk controls with plans. Review is the systematic measurement of whether or not, the benefit was worth the cost.

Operational Risk Management provides a logical and systematic means of identifying and controlling risks. It offers organizations a powerful tool for increasing effectiveness and reducing mishaps.

PROVISIONING FOR OPERATIONAL RISKS

As per Basel II accord, banks sooner or later, will have to quantify their operational risks and provide the regulatory capital for this, in their balance sheet. Provisioning for operational risks is a little different from provisioning for credit and market risks, in the sense that the latter is more predictable than the former. For example, if the loan becomes bad because of certain defined parameters, it can be predicted that the loan will not be repaid by the debtor and the banks will therefore, need to provide for it. In case of operation risks, it will be difficult to predict whether there will be an earthquake/ flood/ system failure, etc. Basel II has of course, suggested a few methods to quantify operational risks and to calculate capital for allocation. These methods are briefly discussed below, in increasing order of their sophistication.

1. **Basic Indicator Approach (BIA):** In this approach, the required capital is determined by multiplying a financial indicator, such as gross income, by a fixed percentage. This approach is easy to implement and is universally applicable to every bank, regardless of its complexity or sophistication. The fixed percentage is basically, a premium for unpredictability.
2. **The standardized approach:** In this approach, the bank's activities are divided into eight business lines. Within each business line, broad indicators are specified that reflect the size or volume of the bank's activities in that area. The total capital charge for operational risk is calculated as, the simple summation of the regulatory capital charges, over the whole business line.
3. **Internal measurement approach:** In this approach, there are the same business lines as in the case of the standardized approach, but an extra dimension, i.e. risk types, is introduced. The capital is calculated

for each combination of business lines and risk types and bank-wide capital is calculated, which is the sum of all these above calculated figures.

4. **Loss distribution approach:** In this approach, banks have to calculate two distributions: one for frequency and one for severity. The aggregate loss distribution can be found by simulating and combining the distributions for severity and frequency of operational losses, over a fixed period of a year, for example. The 99.9 percentile from the resulting distribution for one year Value at Risk (VaR) is then estimated, which gives the capital charge
5. **Scorecard approach:** In this approach, an initial level of operational risk capital is set, and then modified, based on scorecards filled out by line personnel, at regular intervals. This approach allows forward-looking assessments, based on improvements in risk control to be reflected in the level of capital. Scorecard approach can be considered as the forecast of operational losses and events that cause them, based on the knowledge of business experts.

Of all these approaches, although the loss distribution approach seems to be more scientific, it suffers from a major drawback, i.e. non-availability of loss data in the bank. Researchers engaged in this area for devising a model for quantifying operational risks, also suffer from the scarcity of appropriate data and even if it is available, banks will rarely make their history of loss data publicly known because of reputation risks.

IS AUDIT CHECKLIST FOR OPERATION CONTROL

Table 9.6 IS Audit checklist

No.	Particulars	Yes	No	Observations/remarks
1.	Physical security			
1.1	Server room/Data centre (DC)			
(a)	Is the server room (DC) easily accessible to unauthorized persons?			
(b)	Is the server room (DC) away from the basement, main water drainage?			
(c)	Is the server room locked and is the key under the custody of an authorized person?			

(Contd)

No.	Particulars	Yes	No	Observations/remarks
(d)	Is/are the server(s) in close proximity to the UPS room?			
(e)	Are activities in the server room (DC) monitored?			
(f)	1. Does the air-conditioning provide adequate cooling? 2. Has a backup measure been provided?			
(g)	Are storage devices kept inside the server room?			
(h)	Are humidity and heat measuring instruments like, thermometer and hygrometer, installed in the server room, are these being used?			
(i)	Is the server room (DC) neat and clean? Is house-keeping done regularly, under the supervision of authorized personnel?			
(j)	Are fire and smoke alarms/indicators installed in the server room (DC)? Are the alarms audible enough, for all concerned?			
(k)	Are these detectors installed in proper locations?			
(l)	Are fire suppressant systems checked regularly, to see if they are in a working condition?			
(m)	Is there video surveillance in the server room (DC)?			
(n)	Do employees or visitors wear identification badges, as per the policy?			
1.2	UPS			
(a)	Is there a separate enclosure and locking arrangement for UPS?			
(b)	Is the UPS kept in the same room where the servers are kept?			UPS should not be kept in the same room as the servers.
(c)	Is the entry to the UPS housing facility, the same as the entrance to the server room?			
(d)	Is the UPS housing facility spacious enough, for the movement of maintenance personnel?			

(Contd)

No.	Particulars	Yes	No	Observations/remarks
(e)	Does the maintenance agency provide battery service, regularly?			
(f)	Are there sufficient environmental controls in the UPS housing facility?			
(g)	Does the UPS cabin have adequate ventilation to take care of acid fumes, emitted by the lead acid batteries?			
(h)	Is the capacity of the UPS system sufficient to take care of electricity load, required by the computers installed?			
(i)	Are the power cords fixed firmly in their sockets?			
(j)	Is the UPS free of load of the tube-lights, fans, water coolers, etc.?			
(k)	Does the UPS function properly when electricity fails?			
(l)	Is there provision for a generator backup, in case of long hours of power black-out?			
(m)	Is the line voltage, monitored?			
(n)	Is the power supply regulated (for voltage fluctuation)?			
(o)	Is an emergency lighting system available?			
1.3	Fire protection			
(a)	Is there a fire suppression system for the server room/ data centre?			The fire suppressants should not be detrimental to the health of the personnel.
(b)	Are fire extinguishers kept in easily accessible locations, in the premises?			
(c)	Are fire extinguishers installed at strategic places like, server room, UPS room, etc.?			
(d)	Has training been provided to the staff, in the usage of fire extinguishers?			
(e)	Are fire extinguishers regularly refilled/ maintained?			
(f)	Are building materials, fire resistant?			
(g)	Are wall and floor coverings, non-combustible?			

(Contd)

No.	Particulars	Yes	No	Observations/remarks
(h)	Has the smoking restriction been enforced?			
(i)	Are fire resistant safes available and are they used for tapes, disks and documentation?			
(j)	Are fire instructions clearly posted?			
(k)	Are fire alarm buttons clearly visible?			
(l)	Are emergency power-off procedures posted?			
(m)	Is an evacuation plan, with assignment of responsibilities, clearly defined and understood?			
(n)	Is there regular fire drill and training?			
	2. Operational security			
	2.1 Automated Operations Facility (AOF)			
(a)	Is the AOF design authorized?			
(b)	Are the parameters authorized?			
(c)	Are change management procedures in place, for changing parameters?			
(d)	Is the integrity of the parameter file maintained?			
(e)	Is the parameter file backed up properly?			
(f)	Are all computer operations covered by AOF?			
(g)	Is there proper access control for interface, between the manual control and automated control?			
(h)	Are regular reports submitted to the IS management?			
(i)	Are log reports verified, for ensuring scheduling?			
	2.2 Roles			
(a)	Is there a segregation of roles, into system administration, database administration and network administration?			
(b)	Is security administration, a specific role?			
(c)	Has the job description for each level, been prepared and implemented?			
(d)	Is the transaction authorization role, separate from the transaction processing role?			

(Contd)

No.	Particulars	Yes	No	Observations/remarks
(e)	Is the system administrator, supervised and controlled, with respect to creation of user IDs at the OS level and application software level?			
(f)	Is there any policy for job rotation?			
(g)	Is rotation of jobs carried out?			
2.3 Consumables				
(a)	Is the operations group responsible for acquiring and distributing consumables?			As per industry practice, the functional group should be responsible
(b)	Does the IS group give inputs on the specification and requirement of consumables, to the group responsible for consumables?			
(c)	Does the IS group advocate and create awareness on the secure usage of consumables?			
2.4 Processing				
(a)	Does a scheduled system exist, for the execution of programs?			
(b)	Are non-scheduled jobs approved, prior to being run?			
(c)	Is the use of utility programs controlled (in particular those, that can change executable code or data)?			
(d)	Are overrides of system checks conducted by operators, controlled?			
(e)	Are exception reports for such overrides prepared and reviewed, by appropriate personnel?			
3. Backup				
3.1 Backup of data and media security				
(f)	Is there a properly documented policy and procedures?			
(g)	Are the backups stored in a secure location, with proper access control measures?			

(Contd)

No.	Particulars	Yes	No	Observations/remarks
(h)	Is the backup technique properly defined?			
(i)	Is there a process for database backup, apart from the system utilities in the database?			
(j)	Is there differentiation between 'backup' and 'archival'?			
(k)	Are the media used for the archival, stored in a secure location?			
(l)	Is the obsolescence of media/ technology addressed in the archival process?			
(m)	Are all floppies/CDs/tapes that are purchased and pertain to OS software, application software and utility programs, drivers, etc. recorded in a register and stored in fire-resistant cabinet, under dual control?			
(n)	Are the hardware, software, operating system, printer manuals properly labelled and maintained?			
(o)	Are latest user manuals of the application software and other end-user packages that are running, available for guidance?			
(p)	Is the daily/weekly/monthly and quarterly backup of data taken regularly, and is it made available, as per policy?			
(q)	Are backup media properly labelled and numbered?			
(r)	Is there offsite storage of one set of backup?			
(s)	Are backup media verified/ tested periodically, by restoring the data thereof, and maintaining a record of the testing?			
(t)	Is there any test bed, for testing the backup?			
(u)	Is testing done on live systems?			
(v)	Are backup media disposed off, after their specified period in use? Are records available, in respect of such verification/ disposal?			

(Contd)

No.	Particulars	Yes	No	Observations/remarks
4.	Technical support and help desk			
(a)	Are there adequate and documented procedures to guide the help desk personnel?			
(b)	Are the help desk personnel qualified and competent for the job?			
(c)	Are procedures followed by the help desk personnel, in their daily activities?			
(d)	Are the average response, resolution and turnaround time, high?			
(e)	Is the size of the unresolved problems high?			
(f)	Are escalation procedures for call logging, being done properly?			
(g)	Are the third-party service provider's services, contracted and guaranteed in the SLA?			
(h)	In case of third-party help desk personnel, have appropriate non-disclosure agreements been signed?			
5.	Input/output control			
(a)	Are there established procedures for control?			
(b)	Are these procedures being adhered to, by the personnel?			
(c)	Is segregation of duties maintained?			
(d)	Is data integrity maintained?			
(e)	Are reports made available on a regular basis? Are the reports accurate and authentic?			
(f)	Does the user department authorize and authenticate the changes that are required?			
(g)	Is program change control monitored?			
6.	Quality assurance			
(a)	Are duty segregations maintained and adhered to?			
(b)	Are industry standard practices being adhered to, by the staff?			
(c)	Are the personnel qualified and competent to carry out the job?			

(Contd)

No.	Particulars	Yes	No	Observations/remarks
7.	Documentation and program library			
(a)	Are there procedures to ensure that all the programs required for maintenance, are kept in a separate program test library?			
(b)	Are programmers denied access to all libraries, other than the test library?			
(c)	Are there adequate controls for the transfer of programs from production to the programmer's test library?			
(d)	Are transfers from the development library to the production library carried out by persons, independent of the programmers?			
(e)	Do procedures ensure that no transfer can take place, without the change having been properly tested and approved of?			
(f)	Is a report, of program transfers into production, reviewed on a daily basis, by a senior official, to ensure only authorized transfers have been made?			
(g)	Do documents exist for frequent and also infrequent operational activities?			
(h)	Are these documents authenticated by the appropriate authority?			
(i)	Is there a proper change management procedure to update the various documents? Is the procedure being followed?			
(j)	Are the processes entailed in the document, as per the contemporary and international industry standards?			
(k)	Are access controls implemented for the documents?			
(l)	Are the documents backed up in a secure location?			
8.	Removable storage media			
(a)	Are proper criteria in place, to choose the type of media?			

(Contd)

No.	Particulars	Yes	No	Observations/remarks
(b)	Is there any relation between the type of media and the type of backup/archival that it is used for?			
(c)	Is the storage media, stored under appropriate access and environmental controls? Is the media labelled properly?			
(d)	Is there any log, of the number of times of use, of the same storage media?			
(e)	Is storage media kept in the same room as the server/equipment from which data has been stored in the media?			
(f)	Is the storage media disposed after its life span is completed? Are formal disposal procedures followed?			

SUMMARY

Operational control is the limiting factor for all other controls. For example, inspite of the best controls implemented in the Information System, if the backup operator does not take backup regularly, the system administration does not adhere to change management procedures, etc., then the entire controls of the IS goes for a toss. So, for an IT-driven organization, operational control acts as an engine. The functional aspect of the operational control comprises of computer operation, i.e. backup, restoration, etc. input/output operation, scheduling, documentation and program library, technical support and help desk, etc. In this chapter, we discussed comprehensively, the control issues related to all these operational functions. There is a paradigm shift in the way the operational function is carried out in the organization. The function which was earlier done manually by the operators, is now performed automatically. Although the work, related to the operators has reduced, because of the implementation of the Automated Operation Facilities (AOFs), popularly called, light out facility, there are other risks, viz. security and integrity of parameter of AOF, which have assumed significance. While discussing various issues relating to computer operations, we stressed on backup, restoration and also, the roles and responsibilities of the system and network administrators. The control requirements for scheduling, input/output operation, removable storage media, documentation/program library and quality assurance, etc. were discussed at length. While deliberating on the technical support and help

desk function, we stressed the need for a Service Level Agreement (SLA) and the control requirements of the SLA, in case this function is carried out by a third-party.

The management requirement for monitoring a third-party operation, was also discussed at length. In the section "physical and environmental control", we discussed various issues related to access control, and utility failures, etc. Briefly, we also summarized the control objectives in COBIT, related to operation control. Lastly, having deliberated at length, on operation control, we could not resist the temptation to introduce our readers to operational risks, and their implications for the banking community, in the light of Basel II. As usual, we also provided a generic checklist of operational controls, at the end.

REVIEW QUESTIONS

1. What is the transformation that has taken place, in the way the operational functions are exercised in an organization? Write in brief about the control implications of this transformation.
2. Describe the operational control issues, related to centralized vis-à-vis decentralized operation.
3. Describe the duties that are required to be performed by a system administrator.
4. Describe the duties that are required to be performed by a network administrator.
5. Describe the control requirements for backup, in an organization.
6. Describe the various backup techniques used by an organization.
7. Describe the control requirements for the documentation and program library function, of computer operation.
8. What are the controls required for the maintenance of removable storage media?
9. What is the purpose of providing technical support to end-users, by operation professionals? Describe various services and the controls required for these services, offered by the computer operation to the end-users.
10. Briefly describe the objectives of the physical and environmental controls, required for the Information System and describe four such controls.

MULTIPLE CHOICE QUESTIONS

1. In conducting the review of an automated operation facility, the IS auditor will give stress to:
 - (a) Access to the AOF.
 - (b) Segregation of duties.
 - (c) Controls for AOF parameters.
 - (d) Backup procedures.
2. Which of the following is NOT the work of a Database Administrator (DBA)?
 - (a) Selecting and implementing database optimization tools.
 - (b) Specifying physical data definition.
 - (c) Backup and recovery of database.
 - (d) Evaluating an appropriate DBMS for the organization.
3. Which of the following criteria is of LEAST importance in evaluating a potential off-site storage vendor:
 - (a) Media management and environmental factor.
 - (b) The number of employees.
 - (c) Reputation and site security.
 - (d) Transportation.
4. Which of the following procedures would MOST effectively detect employee loading of illegal software packages, onto a network:
 - (a) Use of diskette work stations.
 - (b) Periodic checking of hard drives.
 - (c) The use of current antivirus software.
 - (d) Policies that result in instant dismissal, if violated.
5. Which of the following can a Local Area Network (LAN) administrator use, to protect against exposure to illegal or unlicensed software usage, by the network users?
 - (a) A software metering.
 - (b) Virus detection software.
 - (c) Software encryption.
 - (d) Software inventory programs.
6. The input/output control function is responsible for:
 - (a) Pulling and returning all tape files.
 - (b) Entering and verifying key data.

- (c) Logging batches and reconciling hash totals.
- (d) Executing both, production and test jobs.
- 7. Which of the following is the MOST effective control for visitor access to a data center:
 - (a) Visitors are escorted.
 - (b) Visitor has to wear badges.
 - (c) Sign-in procedure for visitors.
 - (d) Spot checking of the visitors by the operators.
- 8. Removable storage media should not remain unused for a long period of time because:
 - (a) The data they contain will become out-of-date.
 - (b) The risk of read and write error will increase.
 - (c) The likelihood of unauthorized access will increase.
 - (d) Becomes difficult to backup that media.
- 9. The purpose of deleting data from magnetic tapes, before the ends are clipped is to:
 - (a) Indicate which section of the tape should be clipped.
 - (b) Protect the privacy of the data.
 - (c) Prevent damage to the data on the tape.
 - (d) Relieve pressure from the tape hub.
- 10. Which of the following is least likely to be the function of a documentation librarian?
 - (a) Ensuring proper access rights to the documentation.
 - (b) Secure storage of documentation.
 - (c) Ensuring backup for the documentation.
 - (d) Ensuring that only authorized persons get access to documentation.
- 11. Sanitization of data from the media means:
 - (a) Degaussing of the data.
 - (b) Overwriting, degaussing and physical destruction.
 - (c) Removing the redundancies from the data.
 - (d) Cleansing of the record.
- 12. Which of the following should not be addressed by SLA, for outsourcing the computer maintenance to a third-party?
 - (a) The qualification of the third-party's engineer.
 - (b) The key performance parameters.
 - (c) Who will measure delivery, and how.
 - (d) Salary paid by the company to its engineers.

13. What will be the appropriate fire suppressant for a light out data center?
 - (a) Carbon Dioxide (CO₂).
 - (b) Water sprinklers.
 - (c) FM 200.
 - (d) Halon.
14. The alarm for a smoke detector in a data center, should be audible to:
 - (a) The fire department.
 - (b) The CEO.
 - (c) The main security personnel.
 - (d) The chief operating officer.
15. The basic difference between a fire extinguisher and an integrated fire suppression system is:
 - (a) Both perform do the same function.
 - (b) Fire extinguisher puts the fire out, but cannot localize it.
 - (c) The fire suppressant system is gas-based.
 - (d) The fire suppressant can only suppress the fire, but cannot extinguish it.

DISCUSSIONS AND RESEARCH QUESTIONS

1. 'Operational control is the engine for the organization'. Discuss in the context of the importance of operational control for an IT-driven organization.
2. Discuss the grand parent-parent-child backup techniques. Also, describe its relevance in the present-day technology.
3. How is the help desk function useful in IS knowledge management? Discuss.
4. Discuss the various controls for a Service Level Agreement (SLA).
5. What is Operational Risk Management (ORM)? Discuss the importance of ORM from a banking perspective.

EXERCISES

1. Write the salient features of a system administration manual.
2. AB Corp is a manufacturing company that has a varied geographical presence. Though they are only a couple of years into the business and have computerized operations, they are now, planning to set up their disaster recovery setup, in another geographical area. To begin with, they

want to have a simple backup facility. The management has instructed all the regional offices to fetch all the data available with them and store them at the backup facility. Now, you as the IS manager have to chalk out a plan for this process. The plan should contain the objectives of the management's decision and should provide specific emphasis on the operational controls that are required to implement of this process.

3. ON-TARGET is an IT company that, as its name suggests, is very methodical in its approach to various issues, and claims to be very organized. But as is with many organizations, there are some small hiccups and the proverbial '*slip between the cup and the lip*'. The company had a full-fledged backup administrator. The backup administrator was taking regular backups of all the servers, applications and databases. Now, you visit the company, by virtue of being an external auditor. Can you find out what could have happened there and list out all that could have gone wrong, with specific emphasis on backup?
4. The clearing house, managed by the Central bank of the country, has devised a Floppy-based Input clearing (FBIC), where the participating bankers will give the data, related to their cheques/instruments, in a floppy to the clearing house. The physical instruments are dropped in a receptacle, meant for the participating bank. The clearing house authority decides the format of the data in the floppy. The president of the clearing house gets complaints from some of the participating banks, about the wrong data given by some of the participating bankers, thereby resulting in wrong debit to some members. While enquiring the matter with the manager of the clearing house, the president of the clearing house was informed that there are administrative procedures for handling such irregularities, by the member banks. On enquiry, some of the member banks raised the issue that the original data in the floppy was directly captured from their banking application, so there is an error at the source. So, the error could have been made by manipulating the data enroute, to the clearing house or by the operating staff at the clearing house. Now, the president calls you as head of the IT audit, to prescribe a short-term solution for the problem and also devise a long-term strategy for ensuring non-recurrence of such irregularities. You are required to give a solution.
5. ABC Bank is a part of a consortium of five banks (B5) for sharing of ATMs. M/s India ATM Co. is the service provider. They are planning to connect their ATM switch with the switch of M/s India ATM Co. The connectivity modes planned, are leased line, as well as VSAT. Initially, for VSAT connectivity, they are planning to connect IDU (Indoor Unit)

of VSAT through a router, with two Ethernet ports, one serial port and 1 ISDN BRI port. As they don't have a router with such a configuration, they are planning to directly connect IDU to a firewall temporarily, till the router mentioned above, is sourced. Write the security implications of such a proposal, from an operational control perspective.

6. You are an Information System auditor in a firm of external auditors and have recently been engaged to undertake the audit of the IS operation of XYZ Bank. As part of your effort to gain familiarity with the Information System of the bank, you went to the IS operational manager and asked him about the backup procedure.

He informs you that the operation staff makes the full backup of the file everyday, on magnetic tape. Backup starts around 7.00 p.m. and the functional transactions are consequently completed. Operator stores the backup in a tape library, which is a locked room near the server room. This library is managed by a part time employee (clerk), in the current account section. Each day, the clerk collects the backup and takes it to another bank (ABC Bank), located a few miles away. There is a reciprocal arrangement between XYZ and ABC Bank to store each other's backup.

Having asked about your intention to enter the library, the operational manager cordially tells you to enter the library. Upon entering the library, without any hassle, you discover that the room is very untidy and a large number of tapes have been stocked on the floor. These tapes appear to be backup files, created on various days, over the past two weeks. Surprisingly, you also find that the backup tapes of ABC Bank are mixed up with these tapes. Accidentally, you also come across a file containing the records of the backup tapes, which is incomplete and does not tally with the stock of the tapes. Moreover, there is no entry in the record, for the last two weeks.

On interviewing the clerk, responsible for the file library, he (the clerk) expresses his helplessness, as he is over burdened and has to do a whole lot of other work. He also tells you that this matter was brought to the notice of the operational manager several times, but to no avail.

On the basis of the above state of affairs, discuss the exposure, that XYZ Bank is facing and give your recommendations for setting things right.

10

Business Continuity and Disaster Recovery (BCP/DR) Planning Control

-
- ❖ Introduction
 - ❖ Need for Business Continuity and Disaster Recovery Planning
 - ❖ Causes of disaster conditions
 - ❖ BCP Lifecycle
 - ❖ Business impact analysis
 - ❖ Recovery strategies
 - ❖ Developing a detailed BCP
 - ❖ Case study of a bank
 - ❖ Audit checklists
-

INTRODUCTION

Does the name of this chapter, ring a bell? Most of you would have heard it at some point or the other in your life and some of you might have been part of this process, without even knowing it. We can safely presume that all of you, well almost all, would have done this in your life, maybe not in the Information System domain, but in some sphere of life. Planning ahead for failures, has long been in practice, in various spheres of life and this has also been incorporated in the Information Systems arena and has been christened *Business Continuity Planning and Disaster Recovery Planning (BCP and DRP)*.

Box 10.1

One of the earliest civilizations was the Egyptian civilization. The Egyptians had a peculiar custom. Upon the death of a king, it was believed that the soul of the king had gone to an unknown “Heavenly Egypt”. It was believed that preserving the body meant the Survival of the soul. Hence, the bodies used to be preserved, after a long-drawn process called ‘mummification’. Not only were the bodies preserved, but all the personal belongings of the deceased king, were placed by his side, for his use. This form of *survival* was one of the precursors to the present-day business continuity and disaster recovery.

NEED FOR BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

From an Information System's perspective, the objective of BCP-DRP is to facilitate businesses, to continue their operations, even in the event of the occurrence of any disaster or major disruption to their Information System infrastructure or any of its components. The need for planning for such kind of eventuality arises because of the following reasons:

- Dynamism of the Information System
- Unpredictability of the disaster
- Dependence of the business on the Information System
- Competitive advantages
- Increased throughput (transaction per second)
- Reputational loss, in case the business does not restore to normalcy after disaster

WHAT IS A DISASTER IN AN INFORMATION SYSTEM?

Although perceptions about what constitutes a disaster in the Information System, differ from organization to organization and depend on the risk-taking capacity and the dependence of the IS on the business, yet there are certain common characteristics of a disaster, i.e. sudden occurrence/unpredictability, disruption of business operations (that stops the organization from providing its *critical & essential services*), that affect the *most important assets* of the organization, etc. Taking all these essential characteristics into consideration, we can now define Disaster as ‘a sudden, unplanned calamitous event that stops

the organization from providing critical and essential services, by affecting the organization's critical resources, i.e. people, information, facilities and technology.

Causes of Conditions of Disaster

As has been already pointed out, disaster is unpredictable and as such, we cannot clearly identify the reasons for occurrences of disasters. However, the various causes which could result in a disaster are as below:

Natural disasters

- Floods,
- Cyclones,
- Fires,
- Earthquakes, etc.

Utilities

- Electricity,
- Water,
- Communications, etc.

Human causes

- Strikes,
- Sabotage,
- Terrorism,
- Viruses.

Equipment failures

- Information Systems,
- Data communications and networking,
- Telecom.

Human errors

- Programmer/operator errors,
- Lost or damaged backup.

Contamination

- Biological virus (Plague, SARS), etc.

An occurrence of these events however, does not essentially result in a disaster condition. The events which will affect the business or the IS resources adversely, are treated as disasters. Sometimes, system malfunctions or viruses can cause disruptions and these would require some corrective actions to be undertaken,

to make the Information System operational. So, these cannot be classified as disasters. Hence, it is absolutely imperative to have a well-defined and risk-based classification system and this system needs to be operational, to determine the initialization of business continuity processes.

BCP VIS-A-VIS DRP

A Business Continuity Plan (BCP) is a statement of the actions to be taken, the resources to be used and the procedures to be followed before, during and after a disaster that has rendered a business function, totally or partially, inoperative. BCP is a *business* plan, wherein the goal is to minimise the loss to the enterprise, in case of a disaster. The BCP document reflects an organization's ability to maintain the *continuity* of *critical* operations, across the business enterprise. This is like a preventive control for the organization.

The Disaster Recovery Plan (DRP) forms part of the BCP. The DRP is usually a plan for the Information System, to recover from a disaster, to a processing facility. The DRP should be consistent with and is a part of the organization's overall Business Continuity Plan. DRP is concerned with the immediate and temporary *restoration* of computing and network operations, after a natural or man-made disaster, within a defined timeframe. DRP is the technological aspect of BCP. Disaster recovery is '*the science of mitigating the impact of disasters, no matter what causes them*'. Unlike BCP, a Disaster Recovery Plan is more of a corrective control for the organization.

Since the Business Continuity and Disaster Recovery Plan are strategic issues and linked with the continuity of the business, these should be approved by the CEO of the organization.

BCP PROCESS

A Business Continuity Plan should take into consideration, all the different types of events that affect the Information System processing facilities and in turn, the normal business operations. For the worst-case scenarios, the plan should have both a short-term, fallback plan and a long-term, permanent plan. This will help in ensuring the continuity of business operations both, in the long, as well as in the short run.

To have an effective and operational Business Continuity Plan, a detailed study should be undertaken. The following are the different phases in the planning process:

- Business Impact Analysis (BIA),
- Developing effective business recovery strategies,

- Developing a detailed plan,
- Implementing the plan,
- Testing and maintaining the plan.

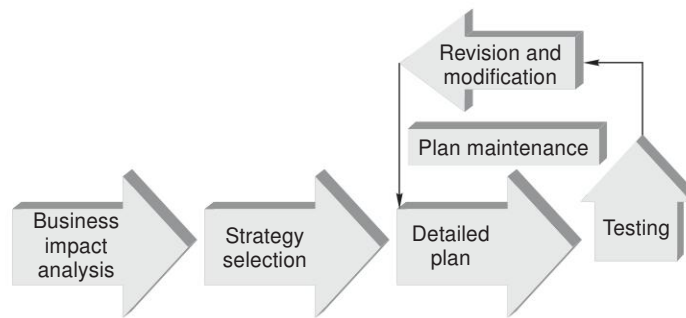


Fig. 10.1 Lifecycle of business continuity plan and audit

Business Impact Analysis (BIA)

This is the primary step in the development of the Business Continuity Plan. This phase identifies the different events that could impact the continuity of business operations, as well as the reputation and financial position of the organization. This phase also quantifies the impact on the business organization, in case of any disruption to the organization's mission critical processes or activities. This phase further identifies, the minimum set of resources, required by the organization, to achieve its Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for its mission critical activities.

Box 10.2

Recovery Time Objective (RTO): refers to the interval of time from the occurrence of the incident (disaster) and disruption system activity, until complete recovery and the resumption of services by the system. RTO is a function of the type of disaster and of the technologies used for recovery. The time period between disruption and resumption of system activity may vary from, a few seconds (for extended clusters), hours or days (for manual migration) to days or weeks (tape restore from recovery site) or may stretch infinitely (failure of two disks in a RAID configuration, where no backup exists)

Recovery Point Objective (RPO): A disaster can result in loss, of online data especially if an up-to-date backup copy of the data is not available.

(Contd)

The point in time, at which data after is recovered after an outage is called the recovery point. High Availability (HA) technologies can be chosen, such that the recovery point will be as close to the instant of disaster as possible. This is the Recovery Point Objective (RPO), required by the enterprise application. It may vary from a few seconds (for Synchronous Replication), to a few minutes (for Asynchronous Replication), to a few hours (for Periodic Replication), to a few days (Tape backup) or may never happen in, case, no steps, taken to protect the data.

There are certain prerequisites, necessary for performing BIA and the foremost among them is, a thorough understanding of the organization. Apart from this, an understanding of the vital business processes, the Information System resources and the human resources, driving these key areas, would go a long way in effectively performing the analysis. The key to a successful BIA, is the recognition of the fact that the BIA should be performed in an end-to-end business context and not on the basis of the individual components that constitute the business. It should be noted, here that this phase must have the approval and support of the senior-level management, since business continuity planning, as has already been mentioned, is the prerogative of the senior-level management. Apart from the support of the management, this phase also involves the widespread participation of personnel from the Information Technology department and the end-users of the Information System. The importance of the Information System resources that drive the critical business operations of the organization, should be established and the planning activity should not be concerned only with the traditional Information System resources. A more expansive plan will make it more holistic.

Different Approaches to BIA

There are different methodologies through which a BIA can be conducted. These include:

- Assessment questionnaires,
- Checklists,
- Interviews,
- A Business Impact Analysis matrix.

There are several proprietary software products available, that can conduct a BIA, but these are not essential for the successful completion of a BIA. Whatever be the approach, it is advantageous to keep the process straightforward and simple. The team carrying out the BIA should comprise, *inter alia*,

business managers who are well-equipped to correctly assess the effects that certain events can have on the continuity of business operations.

One of the most popular approaches, is the 'assessment questionnaire approach'. In this approach, the development of the questionnaire, is the key. The questionnaire should encompass all the functional business areas and should be very lucid. It should be accompanied by a set of instructions, on how to complete the questionnaire. The questionnaire should then be circulated to the key users of the Information System, as well as among the end-users.

Upon receiving the completed questionnaire, the information gathered, is tabulated and analysed. Upon analysis, if it is found that some more information is necessary, then the BIA team should contact the relevant personnel and get the required information. This can be done through structured interviews, to get the desired information. A strategic plan can be developed after the completion of this analysis.

Some of the questions that need to be considered are:

- What are the vital Information System resources that are directly related to the organization's critical business processes? This question is of paramount importance, because not all disruptions to the Information System can be classified as disasters, unless a particular information resource is directly linked to some vital business process and can cause revenue loss to the organization in case of disruptions to it. While the criticality and importance of the business processes varies from business to business and from one organization to the other, there are certain indicators which serve to identify the importance of business processes to the organization. Some of the indicators are:
 - The process supports human lives, health and safety,
 - A disruption in the process, results in financial and/or reputational loss to the organization or increases the cost of operations (through some other means), beyond acceptable limits,
 - The process must satisfy regulatory and statutory requirements.
- What is the critical duration, within which the Information Systems should resume business processes, before unacceptable loss is suffered? The answer to this question, will vary from organization to organization, based on the business that a particular organization is involved in. For example, if the organization is into a business, concerned with satellite operations, then the time period for recovery cannot be more than a few minutes, because with each passing

minute, the loss increases exponentially! In case of a bank, the recovery window for critical banking operations is longer, but cannot be more than a day. If you take the example of a manufacturing firm, then the disruption can be tolerated for much longer, than in the case of a bank.

It should be noted here, that in each example stated above, the recovery window cited, that which is acceptable, only under standard conditions. The recovery window may vary, depending on various factors like the season, time, etc. For example, an ice candy manufacturing unit can afford a longer recovery window in winters, than during summers; while a bank can similarly, afford a longer recovery window on a Saturday, than on a Monday or any other weekday (assuming that the bank is closed on Sunday).

- What is the systems risk ranking?

Outcome of BIA

The following are some of the key outcomes of a successful BIA:

- Identification of organization mission objectives and outputs (in terms of services and/or products, etc.),
- Mission critical activities, their dependencies and inter-dependencies and single points of failure,
- Impact (both, financial and non-financial) and consequences, arising out of disruption/interruption or loss of mission critical activities,
- A minimum, acceptable resource recovery option that is required to enable bare minimum continuity of business,
- Various constraints on critical resources and other vital data.

Recovery Strategies

The next phase in the development of the BCP is to identify, determine and select the most appropriate strategy, from among the various recovery strategies that are designed to help recover from a disaster. A recovery strategy, as the name implies, is a means by which, a system can recover, in case it is struck by disaster. Depending on the system and various other conditional parameters, there can be more than one recovery strategy, associated with the recovery of a system and some strategy might be better than the others, in certain situations. The team that develops the BCP-DRP, plan is advised to present each and every recovery strategy to the senior-level management, along with a report on

the circumstances under which each strategy would prove to be the best. It is then, the prerogative of the senior-level management to choose the most appropriate strategy. It should also be noted that the management can decide to employ more than one recovery strategy, when disaster strikes.

Now, after having chosen the recovery strategy, a detailed plan should be prepared, that takes into account the parameters associated with the chosen recovery strategy/strategies.

Before we proceed with an explanation of the plan, let us delve deeper into the following:

- What are the different levels of strategies?
- What are the criteria that should be used for selection of a recovery strategy?
- What are the alternatives?

Different Levels of Strategies

There are 3 levels of strategic planning that need to be considered:

- Organization-wide BCP strategy,
- Process level BCP strategy,
- Resource recovery level BCP strategy.

The reasons for this three-pronged approach to strategic planning are the dependencies, inter-dependencies and single points of failure of critical business processes, as well as, the ability of an organization to provide an alternate source of business processing, in the event of catastrophic failure of some mission critical activity.

Organization-wide BCP Strategy

This strategy defines the highest level, within which all the BCP activities of the organization are aligned with each other. This strategy is usually (mostly), developed as an afterthought, by most organizations, when there are already many approaches in existence. This strategy is a cohesive framework that binds all the other approaches into an integrated BCP framework. This strategy also defines the various conditions and other parameters like, work area, etc. within this framework and these are agreed upon by the senior-level management at the development stage itself.

Process Level BCP Strategy

This constitutes the core of any approach and also addresses, the mission critical activities and processes of the organization. The present trend among

organizations is to define their mission critical activities, in terms of the products and services that they offer. In addition, mission critical activities are now, also part of the systemic processes that are critical to customer service and are also responsible for the stability of the organization, in particular and the industry, in general. This differentiation is not only important for the entire BCP process, but also provides a clear indication of the significance of strategic planning.

Box 10.3

An example of the need for a process level BCP strategy is the Clearing House Automated Payments System (CHAPS) that provides for same-day, high-value, financial payments processing, within the financial services sector. In consequence of the complexity and settlement coupling of CHAPS, there is a specific and detailed BCP strategy for the payments clearing system alone. A generic BCP strategy is simply not strong enough for a process, where failure would cause severe liquidity problems and shake consumer confidence in the financial services industry. (Source: Business Continuity Institute)

Resource Recovery BCP Strategy

This strategy provides the actual, practical link between the BIA and the development of the BCP. This strategy defines the actual approach to the allocation of resources, as a part of the BCP. Resource allocation needs strong commitment from the senior-level management and the strategies should reflect this.

Criteria for Selection of a Recovery Strategy

The selection of a recovery strategy depends on the following criteria:

- Criticality of the business process and its dependencies,
- Cost,
- Time required to recover,
- Security.

From among the various recovery strategies available, the most appropriate recovery strategy would be the one that satisfies, within acceptable limits, the criteria mentioned above.

- The *criticality of a business process* depends on many factors, the foremost amongst which, is the type of business and revenue

percentage that a process contributes to the overall business of the organization. This can also be gauged from the BIA report that contains all the information about various critical business processes of the organization.

- The *cost* of preparing the organization to deal with likely disruptions or interruptions includes, the cost of making purchases, maintaining inventory and regular testing of inventory, maintaining alternative operational work areas, alternative paths for network flow, etc. This cost, together with the cost of making all the aforementioned, operational (in the event of a disruption), is the cost of recovery. The costs for making these operational, can be insured against, but not the costs for preparation.
- The *time* required to recover from a disruptive phase is another key factor and this in turn, is linked to the criticality of the business process. But logic dictates that the lower the time of recovery, the better and more effective the strategy.
- *Security* is another key factor, which is generally overlooked, when it comes to recovering from a disaster. It should be remembered that a disaster causes/enables loss of security. Hence, it is imperative for the recovery strategy, not to lose focus on security, in its endeavour to restore operations.

Alternatives

As is with everything in our daily lives, in the world of Information System too, various alternatives to developing any level of BCP strategy, are available. Also, depending on the industry in which the organization is operating, there will be different options available. Some of the standard alternatives are:

Processing Transfer

This refers to the diversion of mission critical activity, to an alternative part of the same organization or to a different organization that is operating, in the same industry. This alternative requires prior planning and approval. Also, in case an organization opts for diversion of critical activity to another organization, then this practice can be established on a reciprocal basis, with formal contracts and proper Service Level Agreements that should be made enforceable and should also be tested, prior to being made available for use. A reciprocal arrangement offers the following benefits:

- Low cost (for both maintenance and operation),
- Easy and timely action to make the activity, operational,

- Easy to configure and use because of the fact that the organizations are in the same industry.

But such reciprocal arrangements also have a downside:

- Service levels are usually not enforceable, unlike in the parent organization,
- Differences in the organizations' individual equipment configuration, may necessitate changes for operations to be effective,
- The load on the equipment increases, which may create a problem in the overall work.

The following factors should be taken into consideration when choosing a facility for an organization, for reciprocal arrangement:

- The reciprocal site should not be situated in the same locality, as that of the parent site,
- The reciprocal site should not be affected by the same disasters (natural) as the parent site and at the same time,
- There should be a reasonable level of compatibility between the parent site and the reciprocal site, in terms of equipment and strategies,
- There should be sufficient availability of resources in the reciprocal facility, to address the need of the parent site, in case of an emergency,
- The facility should be tested regularly, for use by both, the owners, i.e. the parent site and the reciprocal site.

Some of the factors that organizations need to take into consideration and agree upon, before they enter into any sort of reciprocal arrangement, include the following:

- Duration (while disaster strikes) of use of reciprocal facility,
- The facilities that would be made available,
- The duration of the lead time, to make the facility operational,
- Whether assistance of personnel will be provided,
- Ease of access to the facility,
- Communication facility at the reciprocal site,
- The frequency of testing the facility for compatibility,
- Whether security (of information) will be addressed
- The type of security that would be provided,
- Whether there will be any downtime for the facility.

Change of Process

The management can decide to change the process, as part of its strategy, within the BCP process.

Change of Product, Service or Function

Just as in the case of a process, a product, service or function can also be considered for change, as part of the process. This strategy/option is applicable, especially in those industries, where the lifespan of the product is limited.

Insurance

Although, technically speaking, this option does not involve any strategy for recovery, nonetheless, it gives some time, for getting the recovery process started and running. This option provides for financial compensation/support, in the unfortunate event of incurrence of a loss. Yet, this option does not provide any remedy for the loss of reputation, loss of market-value, loss of customer confidence and damage to the brand image. This is usually called business interruption insurance and is provided, after a detailed BIA has been performed. The BIA has to be done on a regular basis, to appropriately evaluate the level of insurance cover that is required.

Recovery from loss or disruption of mission critical activities, by providing for bare minimum, acceptable levels of continuation, during the period of recovery is another alternative. For infrastructural facilities and processing sites, in case of disruptions, there are many options available. These have been listed below:

Hot Site

A hot site is a processing facility that is usually, kept on standby and made available within a short time span, after disruption to the main processing facility. A hot site is usually, a mirrored replica of the main site, complete with all the equipment, systems, network and software, maintained in a working condition. The only major requirement at a hot site would be staff that is well-versed with the operations at the main site. Most of the times, a hot site would become operational, automatically, the moment activity at the main site is disrupted. Sometimes, its operations can also be controlled, manually.

The costs incurred in getting a hot site operational, can be compensated by the insurance coverage for the main site, if there is proper planning. A third-party hot site can also be subscribed to, in cases of drastic disruption. The cost, associated with such third-party hot sites, varies from vendor to vendor. Generally, vendors charge subscription fee, monthly fee, testing charges, activation costs, etc. The use of the hot site is again, decided by vendors, some

of who allow the hot site to be used on a regular basis, for load sharing purposes, which is not recommended. However, if the hot site is owned by the organization, then, its use, for occasional load sharing or using it on a test basis, is acceptable. While entering into a contract with third-party vendors for hot sites, factors like, the amount of time needed, the frequency, etc. should be decided at the agreement stage itself.

Generally, a hot site is not intended for long-term periods. The hot site should be viewed, only as a means of accomplishing continuation of critical business operations, for the period during which recovery of the main site is being carried out. This duration should also, not extend beyond the agreed recovery time and should conform to the Recovery Point Objectives.

In cases where network connectivity to the hot site is required, the Disaster Recovery Plan should address these issues, as well as those related to maintaining redundancy and capacity on the network paths. Appropriate care should be taken, to avoid any single points of failure, in the use of the hot site.

Warm Site

They are usually, partially configured sites or sites with some minimum infrastructure that can become operational, once the required equipment is put in place (usually a simple piece of equipment or network cable, etc.). Also, most of the times, a warm site requires some form of human intervention to make the facility operational. The maintenance cost, involved in a warm site is much less than that of a hot site. The trade-off for this, is borne by the time factor.

Cold Site

A cold site is akin to a skeletal framework that requires much equipment, configuration, etc., for it to become operational. Usually, a cold site takes several days, before it can gain operational status because of the large volume of equipment and facilities that it requires.

Duplicate Information Processing Facility (DIPF)

Such sites are dedicated, self-developed recovery sites, where the data backup, is almost synchronous with that at the primary site. The recovery time, involved in such sites is very low. These sites can act as stand-by hot sites or maybe reciprocal agreements with another company. The critical issues for maintaining Duplicate Information Processing Facilities are as follows:

- Due to synchronous backup, there will be a constraint on primary processing,

- The DIPF should not be subject to the same natural disasters, as original sites,
- Compatibility must exist and be maintained, between the primary site and DIPF,
- Testing of DIPF is essential, even if it is under the common ownership,
- Sometimes, the primary operation should be shifted to the DIPF, for testing its compatibility with the primary site.

Developing a Detailed Plan

Once the strategies, alternatives and options have been debated and decided, it is time now, to frame the detailed plan. This plan should address, all the issues and factors involved, in recovering from a disaster, ranging from pre-disaster preparedness to post-recovery operations and resumption of normal operations. The factors are as follows:

- Pre-disaster preparedness,
- Evacuation procedures,
- How to declare a disaster,
- The power (authority) to declare a disaster,
- Identification of the business processes and IT resources that need to be recovered,
- Identification of responsibilities, when this plan is in force,
- Clear definition of functional roles in the plan,
- Lucid and elaborate explanation of the recovery alternatives,
- Identification of resource requirement for implementing the plan,
- The procedures for testing the plan,
- The actual implementation,
- Post-recovery testing and operations,
- Total recovery and normal operations, i.e. the declaration of, the end of disaster time operations and resumption of normal operations, after full recovery.

The plan should be written in simple and lucid language and should be easily understandable. A copy of the plan should be maintained, offsite. One of the major tasks in drafting the detailed plan is the assignment of responsibilities to the team members, during various stages of disaster recovery. Also, to implement the plan, key personnel should be identified. Usually,

these key personnel should lead the teams that are prepared, in response to disruptions in a critical function, defined in the plan. The size of the team will depend on the size of the business operation and in some cases, can also be composed of a single person. Mentioned below, are some of the standard teams that can be formed by an organization, during disaster recovery.

- **Emergency action team:** This is the team that should respond first, in case of disasters. Some of the primary tasks that this team should carry out include, evacuation of personnel, securing human life, trying to extinguish fires and dealing with other emergency response scenarios.
- **Damage assessment team:** This team assesses the extent of the damage that has occurred, following the disaster. This team should have the requisite skill and ability to determine the extent of damage, as well as to estimate the time required to recover from the calamity. This team should also be skilled in the use of safety regulations and procedures, while carrying out the damage-determination exercise. The team should also assess the possible causes of the disaster (especially in cases where the disaster is not a natural disaster).
- **Emergency management team:** This is one of the most important teams. This team handles all the coordination activities, of all the other teams, involved in the recovery exercise. This team is responsible for all the key decisions, taken and also determines the activation of the Business Continuity Plan. It is the leader of this team who actually declares that the disruption that has occurred is a disaster and sets the Business Continuity Plan rolling. Apart from this, the other functions of the team include, arranging finances for recovery, handling media and public relations and other legal matters, pertaining to the disaster. This team should also coordinate the following activities:
 - Retrieving critical and vital data from offsite storage,
 - Getting the recovery site (hot site, warm site, cold site) ready, to commence operations,
 - Handling logistics at the recovery site,
 - Operating from the recovery site,
 - Re-establishing communications and network traffic,
 - Arranging logistics for employee relocation, and coordination of work schedules.
- **Offsite storage team:** This team is responsible for the procurement, packaging and the transportation of records and media from the

offsite storage location. This team also coordinates and establishes procedures for offsite storage of information, created during processing, from the recovery site.

- **Software team:** Restoring systems, testing the working of the operating system, resolving system-level problems, restoring essential services for the application environment, etc. are the responsibilities of this team.
- **Applications team:** This team restores the application suite and the requisite service packs, to the systems and monitors the application performance and database integrity.
- **Security team:** This team continuously monitors the security of the system, the subsystems and the packages and resolves any security conflict that impedes the fast recovery of the system.
- **Operations team:** This team coordinates the shifting, installation and operation of the hardware and associated peripherals, at the recovery site. The major task is to coordinate the operations at the system recovery site, manage operations, during the entire duration of the disaster and supervise these operations.
- **Network recovery team:** This team is responsible for the appropriate routing, re-routing, etc. of the network connections and traffic, and establishing network control at the recovery site, while providing continuous support for communications and ensuring the integrity of the communications.
- **Communications team:** This team co-ordinates with the network recovery team and establishes the requisite communication hardware and also liaises with the local telephone exchange and gateway vendors, to ensure continuous access and service.
- **Administrative support team:** This team provides clerical support to the other teams and also serves as a message centre for the entire recovery site.
- **Facilities management team:** This team manages the accounting, payroll, as well as other facilities, for the users at the recovery site.
- **Salvage team:** This team takes a more detailed look at the impact of the disaster and reassesses the damage to equipment and facilities. This team provides the emergency management team detailed input, to determine the viability of relocation of the main site or its reconstruction. Also, details pertaining to insurance claims and salvaging of records (both, paper and electronic) is managed by this team.

- **Relocation team:** This team coordinates the process of shifting from the recovery site, back to the restored main site or to a new site (relocation). The relocation of Information System processing, the operations and the communications, are all managed by this team. The monitoring, of return of the service levels to normalcy, is also the duty of this team.

Some other key areas that require attention and clear mention in the plan, include the following:

Some of the major components include, the list of key decision-making personnel with their contact numbers, a complete list of emergency contact numbers of key personnel who may either be employees of the organization or belong to third parties, vendors, etc. a list of available resources, a list of backup of critical supplies, the organization policy, the communication networks, the tasks assigned to team members, insurance details, Detailed, up-to-date procedures, easily understood by staff members or contract personnel, recruited for dealing with the disaster.

Telecommunications are all pervasive and it is really hard to imagine any business that doesn't use telecommunications in one way or another, whether for simple connectivity of geographically spread-out locations or for ensuring the completion of critical business processes. Ensuring continuous and effective telecommunication capabilities, should be given high priority.

Though telecommunications are susceptible to the natural disasters and other risks that also threaten normal data centres, it should be noted that there are certain risks, which are specific to telecommunications. These risks should also be taken into consideration, while drafting the BCP. Also, such risks are beyond the control of the organization. Some of the risks are telephone exchange disasters, link failure due to cable disconnection malfunctioning of communication software, etc. Though, technically speaking, the service provider's local exchange is responsible for the malfunctioning of communication channels, it is the prerogative and responsibility of the organization to ensure continuous connectivity, while also ensuring sufficient backup that can be used, in case of emergencies. Some of the mechanisms that an organization can use, for protection of its network resources are:

- Redundancy through surplus capacity that could be used in times of emergency,
- Redundancy through multiple paths,
- Redundancy through failover mechanisms, to prevent single point failures in aggregating devices,

- Redundancy through backup measures like, backing up configuration files, etc.,
- Redundancy through multiple service providers, using different communication media, so that disruptions in one media, may not affect an other.
- **Alternative routing:** This is a method of routing data, through an alternate medium, in case of non-availability of the normal network. Some examples of this are, dialup networks and microwave communication, in case of non-availability of dedicated circuits or leased land lines.
- **Diverse routing:** This is the method of routing network traffic, through split cable or duplicate cable facilities. The subscriber can duplicate the facilities by having alternative routes, but the entrance to and from the subscriber's premises may be in the same conduit. Though the subscriber can avail of dual entrance facilities, this will depend on the service provider. This kind of routing is costly, as well as time-consuming.

Another important parameter is the server, which is one of the most critical information processing equipment. The plans should include measures to ensure continuous server operation and also to prevent the server from going offline, for any extended period of time. Providing for fault-resistant, fault-tolerant and failover capabilities, should also be considered. Some of the common mechanisms that are available for providing such capabilities are Redundant Array of Inexpensive Disks (RAID), Fault-tolerant servers, Clustering, etc.

Redundant Array of Inexpensive Disks (RAID) is the technique of breaking up information and writing it across multiple disks, to improve performance, while also improving the read/write/save functions of large files. This can be done using hardware or software.

There are different levels of RAID. Each level and its features are given in Table 10.1

Table 10.1 Levels of RAID

Level 0: Striped disk array, without fault tolerance.	• One disk, out of several, separate physical disk drives, • Improved performance, • Maximum transfer rates, • The read operation can become, several, simultaneous, separate disk reads, of several physical disks, • No redundancy or parity.

(Contd)

510 *Information System Audit and Assurance*

Level 1: Mirroring.	• An exact copy of information, • Disk mirroring, issues, • Mirroring to drives, run from the same controller, does not protect the data from drive-controller failure, unless mirroring to a disk is run from a separate controller, • For higher disk-read performance and greater fault tolerance, a separate disk controller, for each half, of a mirror set, should be used, • Disk mirroring, effectively cuts available disk space, in half, • Low initial cost, • Slows down the writes, • Speeds up the reads, • For multi-user environments, mirroring gets the best performance of all the RAID levels.
Level 2: Hamming code ECC.	• Interweaving data, across multiple drives, including parity information created, using the hamming code technique, • Large number of disks for user storage, • Error recovery coding, • Seldom used, because of the extensive amount of resources needed.
Level 3: Parallel transfer with parity.	• Byte-level parity on a dedicated-drive, • Stripe user data, across multiple drives, • Improved performance, using disk striping, • Dedicated parity drive, • Fault tolerant capabilities, through the availability of redundant drives.
Level 4: Independent data disks, with shared parity disk.	• Similar to Level 3, but uses block-level parity and disk striping, rather than byte-level, within a block.
Level 5: Independent data disks with distributed parity blocks.	• Stripes both, data and parity information, across multiple drives, at the block level, • Data from a parity stripe is recoverable, • Data is written across all striped disks, in a disk array, • Parity information is written to a disk, • On a disk, separate from the one, where the data it corresponds with, is written,

(Contd)

	• Data on that disk can be reconstructed from the parity information on the other disks, • Level 5 is faster than Level 4.
Level 6: Independent data disks, with two independent distributed parity schemes.	• Similar to RAID 5, • It differs, in that, it calculates two sets of parity information, for each block of data.
Level 7: Optimized asynchrony for high I/O rates, as well as, high data transfer rates.	• Asynchronous I/O transfers, • Transfers are independently controlled and cached, via a real-time OS-embedded array control micro-processor, • Highly expensive proprietary solution, providing high performance levels.
Level 10: Very high reliability, combined with high performance.	• Striped array with high I/O rates, achieved by striping, level 1 segments.
Level 53: High I/O rates and data transfer performance.	• A striped level 0 array, with segments, as level 3 arrays, • Expensive solution, • High performance.
Level 0+1: High data transfer performance.	• Mirror array, whose segments are level 0 arrays, • Fault tolerance, similar to level 5, • Very expensive.

In comparing the above techniques, RAID levels 0 and 1, have better performance when they are software-based, whereas RAID levels 3, 5 and 6 run faster on hardware. RAID level 2 is hardware-based and resource-intensive and therefore, is seldom used. The remaining levels are high-cost/ high-overhead solutions, with limited scalability.

Another important parameter is the power supply to all the critical installations. Wherever required, telecommunication equipment should be supplied with power, either through the normal connection or through the Uninterruptible Power Supply (UPS).

It should be noted, that this plan must be consistent with the overall Business Continuity Plan of the organization. In case the organization does not have a well-defined Business Continuity Plan, then the IT Business Continuity Plan can be extended, to include the business units that require some kind of information processing. The plans should include information

on, user areas, information sources, transmission of data for processing, delivery and deployment of the processed results.

Testing and Maintenance

The foremost point to remember here, is that the tests carried out on the Business Continuity Plan will definitely fall short of being full-scale operational tests, due to their very nature and the circumstances under which the tests are carried out. This however should not prevent the BCP from being tested, because testing will bring to light the degree of effectiveness of the plan and will thereby, allow for improvements to be made, if required.

The testing of the BCP should endeavour to accomplish the following tasks:

- Evaluation of the completeness and accuracy of the Business Continuity Plan.
- Evaluation of the performance of the personnel involved in the test,
- Evaluation of the coordination between the BCP team members and third-party vendors.
- Evaluation the performance and the ability of the recovery site to perform the requisite processing,
- Evaluation the preparedness of the equipment, at the recovery site,
- Evaluation of the overall performance, in terms of maintaining business continuity.

There are three types of testing which can be done. They are:

- **Paper test:** This test is a virtual walkthrough of the plan, with all the key personnel, involved in the execution of the plan, figuring out what would happen in various situations. This test, usually precedes the preparedness test.
- **Preparedness test:** This test is usually, a localized version of the full test; a simulation. Different aspects of the plan are tested regularly and this provides an insight, into the efficacy of the different aspects of the plan.
- **Fully operational test:** This test is usually done, after the above two tests are completed. For the purpose of testing the plan, this is the disaster and all the aspects of the plan are tested, in this full-scale testing.

The testing is completed over three phases, each of which, is explained below:

- **Pre-test:** This phase is concerned with, the set of actions that need to be taken, to conduct the actual test. Getting the logistics ready for the conduct of the test, preparation of the recovery site, etc., are the actions to be undertaken, during this phase. While this phase is necessary only, in the testing scenario, it should be noted, that no disaster comes announced and hence, this phase is not part, of what would actually happen, in case of an emergency.
- **Test:** This phase comprises the actual testing of the BCP. All the activities are executed to assess the specific objectives of the BCP. While all the action is taking place, evaluators are at hand, to review the performance of all the parameters, specified earlier. The way the test shapes up, reflects the actual preparedness of the organization for a disaster.
- **Post-test:** This is the cleanup phase; where all the used equipment are returned to their previous position, and the various inputs gathered, while doing the testing, are accumulated. A formal evaluation of the plan is also done.

During each and every phase of the testing, detailed documentation should be carried out on the observations, the problems, the resolution of the problems and improvements that can be made in the plan for that phase. This documentation will go a long way, in the detailed analysis of the testing, while revealing the strengths and weaknesses of the plan.

Analysis

The test results, should be analysed in a holistic and quantitative manner. Some of the common parameters used, to help gauge and analyse the results, would be:

- **Time:** The time taken to complete the tasks from the pre-testing phase onwards, for each process.
- **Amount:** The effort and the amount of work, put in by the personnel, in completing the tasks and processes, assigned to them.
- **Accuracy:** The accuracy of the results of the processing work, done at the recovery site, as compared to similar work, done under normal circumstances.
- **Preparedness:** The alertness, alacrity and vigilance shown by the personnel, responsible for handling the actions to deal with any eventuality.

- **Awareness:** The awareness of the users, regarding the procedures to be adopted, during the actual working of the recovery site operations.

Maintenance

The BCP should not be a stagnant document. It should be reviewed and updated on a regular basis, to reflect the changing requirements and business process methodologies. Given below, are some of the factors that necessitate revision and review of the BCP-DRP:

- A change in time, may change the efficacy of a previously effective strategy,
- A change in the underlying technology,
- A change in an application or a business process,
- The additions of new modules, to existing applications or addition of new applications,
- A change in the management perception of critical processes and practices.

The responsibilities for the maintenance and review of the BCP-DRP document, should include the following:

- Preparing a schedule for review and maintenance,
- Responding to significant changes, apart from the scheduled review,
- Reviewing the comments and observations from the testing change, and incorporating the necessary changes,
- Participating in the scheduled tests and evaluating the adequacy of the plan,
- Preparing a schedule for the training of personnel, in emergency and recovery procedures,
- Ensuring the maintenance of revised plan documents, in the scheduled areas,
- Ensuring the completeness of the document, in all respects.

DATA BACKUP/STORAGE

The most important thing for any kind of Business Continuity and Disaster Recovery planning, for an Information System, are successful/efficient backup procedures. Some of the important control issues, related to the above, are discussed below:

Storage Media

Various secondary storage media, are used to store programs and associated data, for backup purposes. A table showing the various secondary media, their capacity, speed and relative longevity, is exhibited below in Table 10.2.

Table 10.2 Secondary storage media

S.No.	Type	Capacity	Speed of data transfer	Remarks
1. Magnetic tape	AIT: Advanced Intelligent Tape	0.5–1.3 TB	30–78 MBps	Better performance than DLT. Higher capacity with SAN (Storage Area Network).
	DLT: Digital Linear Tape	Up to 80 GB	12 MBps	Reliable and inexpensive. Mostly used in mid-sized server/network.
	DTF: Digital Tape Format	Up to 518 GB	24 MBps	With SAN, can reach upto 18 TB. Good for data centre.
	DAT: Digital Audio Tape	Up to 40 GB	3 MBps	Good for mid-sized server/network scenario.
2. Optical	CD: Compact Disc	650 to 900 MB	6 MBps	Depending on type (R/RW/ROM), offers 1000 rewrites.
	DVD: Digital Versatile Disk	4.7 to 17 GB	6–12 MBps	Depending on type (R/RW/ROM), offers 100000 rewrites. Highly used on stand-alone systems.
3. Magneto hybrid		Up to 9 GB on disks (similar to floppy)	4 MBps	optical With SAN, can give higher capacity.

(Contd)

516 *Information System Audit and Assurance*

S.No.	Type	Capacity	Speed of data transfer	Remarks
4.	Magnetic disk	Up to 2 GB	5.5–12 MBps	Expensive. Only for general purpose storage.
5.	Floppy disk	1.44 MB	0.06 MBps	For daily use. Old technology.

These secondary storage media, are stored in one or more physical facilities, referred to as offsite libraries. Controls over offsite libraries/ location, are very important for integrity of the data and its consequent recovery, in case of a disaster. The various controls, over the offsite library, are discussed below:

- Physical access to the offsite library and location should be secure, as in the case of the originating site,
- The offsite facility should possess the same constant environmental monitoring and control, as the originating site,
- The offsite facility should not be easily identifiable from outside, i.e. there should not be any signboards,
- The offsite library should have a detailed list of inventories of the media and a proper record should be maintained for the media/ files that are moved into and out of the library,
- The offsite location should have a copy of the backup procedures.

Data Replication

Data replication technologies, mirror data from one storage disk to another, in real time, over high bandwidth, dedicated networks. The issue of application of this technology, should be decided in the planning phase itself. Data replication can be of three types:

- **Synchronous replication:** In this mode of replication, block-level data transactions or I/O operations, are committed to one or more remote storage systems, prior to sending a write acknowledgment, back to the primary unit. The host application is not allowed to proceed, until the data is successfully committed to all storage systems. This requires a high network bandwidth and low latency.
- **Asynchronous replication:** In this mode of replication, I/O operations are written to the primary storage system and then, sent to one or more remote storage systems, at some later point in time.

The host application functions as usual, unaware of whether or not the data has been written to the remote storage systems. The replication can be scheduled for a time, when the network bandwidth is high and latency is low, thereby, optimally using the network connection.

- **Semi-synchronous replication:** This is a hybrid approach, wherein, I/O operations are written on the primary storage system, the application is allowed to proceed, and the data is in the meanwhile, synchronized with the remote storage systems, with a minimal time lag. Here also, bandwidth and latency are important issues to be considered.

Box 10.4

Replication of Oracle database redo log

A redo log is present for every Oracle database and it records all the changes made, in an Oracle database. It is usually, referred to as, the '*online redo log*'. It consists of at least two redo log files, that are separate from the data files. In case of any failure (media or instance), Oracle applies appropriate changes, in the redo log of the database, to the data files, which update data in the database, to the instant when the failure occurred. An Oracle database can operate, either in 'archive log' mode, or 'no archive log' mode. In archive log mode, the redo log files that are generated, are also archived. Database recovery from media failure is possible, only if the database operates in the 'archive log' mode. An important point to note, is that *online redo log files must never be copied, when a database runs in archive log mode*. Oracle writes to the redo logs, prior to committing the transaction to disk. Log-based replication, begins reading from the redo logs, as soon as a transaction begins to be recorded. The log-based solution can replicate data, without extensive CPU and network bandwidth usage. This log-based solution, maintains the Oracle read-consistency model, so that the replica is an accurate representation of the primary database. This form of data replication, allows the primary and secondary databases to operate independently, running different versions of Oracle, on different operating systems. The failover procedure, with this solution, does not include downtime for database recovery, i.e. an instance of the database is always running and is accessible.

Data Storage

Using multiple storage systems, prevents single point failures. Also, using multiple storage systems that are spread geographically, across different areas, prevents loss of data during disasters. The methodologies and technologies that would be used in storage and replication of data, should be decided in the planning phase. Some of the prevailing storage-networking options, for interconnecting multiple data centers, include:

- **Dense Wavelength Division Multiplexing (DWDM):** DWDM gathers data from different sources and protocols, on an optical fibre, with each signal, carried on its own separate and private, light wavelength. DWDM technology can multiplex upto 80 (practically and, theoretically, even more) separate wavelengths, carrying data into a light stream, transmitted on a single optical fibre, providing a cost-efficient utilization of an enterprise's network resources. DWDM is well-suited for natively (no protocol conversion) extending, Storage Area Networks (SAN), in cases where multiple communication links or channels are required. Data replication, over several hundred kilometres, is supported.
- **Synchronous optical network (Sonet):** Sonet technology is based on time division multiplexing, where traffic from multiple subscribers, is multiplexed together and sent out, onto the network, as an optical signal.
- **Storage over Internet protocol:** Storage over IP, enables transportation of block-level storage, over an IP network via, protocols like, iSCSI, FCIP (Fibre Channel over IP) or iFCP (Internet Fibre Channel Protocol). Data rates are usually, around 155 Mbps. Storage over IP, enables storage traffic to extend great distances via, a variety of wide area networking options such as, T1/E1 and T3/E3 circuits, Asynchronous Transfer Mode (ATM), frame relay and Ethernet. Synchronous or semi-synchronous mirroring may be difficult, because of the higher, less predictable latencies, associated with IP networks.
- **Storage Area Network (SAN):** A SAN is a high-speed sub-network, of shared storage devices and their associated servers, i.e. a network dedicated to storage. The architecture relies on a dedicated fibre (sometimes SCSI is also used) network, rather than an Ethernet LAN, to make the connection. This architecture works in such a way that makes all the storage devices, available to all the servers on a LAN (Local Area Network) or WAN (Wide Area Network). As

more storage devices are added to a SAN, they too will be accessible, from any server in the larger network. In this case, the server merely acts as a pathway, between the end-user and the stored data. Since the stored data does not reside directly, on any of the network's servers, the server power is utilized for business applications, and network capacity is available to the end-user. Such an architecture, allows for integrated data management and efficient data-sharing, in a heterogeneous server environment. Some of the major advantages of a SAN are:

- High scalability
 - High system availability
 - Extensive fault tolerance
 - Low cost of ownership
- **Network Attached Storage (NAS):** This is a data-centric storage architecture, that provides file storage over a network (usually, within a LAN), using file access network protocols like, NFS, etc. A NAS device is usually, a dedicated device and does not provide any of the activities that a server in a server-centric system, typically provides. The server only does the processing, while the NAS device, handles storage, and delivers data to the users. A NAS device, or multiple networked NAS devices can exist anywhere in a LAN. The consolidation of storage resources, provides simplified management and scalability.

Table 10.3 Difference between SAN and NAS

S.No.	SAN	NAS
1.	Dedicated storage network.	Dedicated storage, over existing network.
2.	Medium is usually, fibre.	Media is copper (Ethernet).
3.	Used more for block-level access.	Used for file-level access.
4.	Also works in a WAN environment.	Works only in a LAN environment.
5.	High availability.	Availability depends on underlying media.

DEVELOPING AN APPROPRIATE DISASTER RECOVERY STRATEGY: A CASE STUDY OF A BANKING ORGANIZATION

The Target Bank

The bank has implemented a core banking solution, in a centralized environment. All other delivery channels, viz. Internet banking, ATM, are also operational. The centralized server, Internet banking web servers and the ATM switch, are located in the bank's data center, at location 'X'. The bank has got its own Wide Area Network, with inter-city links, connecting 25 cities, across the country.

Requirement

To develop an appropriate disaster recovery strategy, for the following applications:

- Core banking solution
- ATM switch
- Internet banking solution

Steps

For developing a disaster recovery strategy, for the above applications, we should first, conduct a Business Impact Analysis (BIA) and then, select a strategy for disaster recovery.

BUSINESS IMPACT ANALYSIS (BIA)

The first step in the BIA study, is to gather information on the following aspects:

- Identification of mission critical business functions,
- Applications, associated with critical business functions,
- Interfaces between business functions,
- Financial and non-financial impacts of the unavailability of the business function,
- Potential alternative workaround procedures,
- Required recovery timeframes.

This can be done, by looking at the various inventories of IT applications, interviewing the core professionals, including the vendor's personnel, involved in the project, and the business process owners. During the study, we should prioritize various business functions, in order to ascertain the timeframe over which, they need to be recovered. As part of this prioritization, we should also assign a *criticality ranking*, say on a scale of 0 to 5, to each function, with 5 being the most critical. The criticality ranking, indicates the severity of the impact on the bank, caused due to the unavailability of a given business function. We should also determine the *outage tolerance* of the key business functions. Outage tolerance refers to, 'the maximum allowable time, for which the bank will be able to operate, without a particular business function being performed, before serious repercussions result. Both, the criticality ranking and the outage tolerance, need to be taken into account for determining the sequence of recovery.

For assigning the criticality ranking, what we also call a system risk ranking, we should analyze the functionality of each area or components, their interdependence and the possible disaster scenario that could emerge.

FUNCTIONALITY OF CBS, WITH INTERNET BANKING AND ATM, AS THE DELIVERY CHANNELS

The core database of the bank's CBS application, is placed at the data center and appropriate backup procedures are in place, to store the backup, in an offsite location. The Internet banking application is a three-tier one, i.e. web server, application server and the database server (CBS has the same database server). There is a middleware application, which is placed before the central database server, which converts the data to the appropriate format, before it is committed to the database, or before it comes from the central database to other channels.

The Internet banking database server, takes care of the offline queries from the Internet and gets refreshed from the central database, at periodic intervals. There is an ATM switch, which is connected to the central database, through the middleware. The ATM switch, is the heart and soul, of the ATM channel. It receives queries from the ATMs, sends these to the respective branches (in case of non-CBS, but computerized branches), and to the centralized database, in case of CBS branches. It also stores the Positive Balance File (PBF), of all the non-CBS, computerized branches, for transactions through ATM, after normal office hours.

The network from the branches, go to the data center, through an aggregation point. Some inter-city connections piggy back on a closed-user network say, INFINET (Indian Financial Network). The network is connected to the Internet, only at the data center.

A pictorial representation, of the CBS set up and of the network is given below:

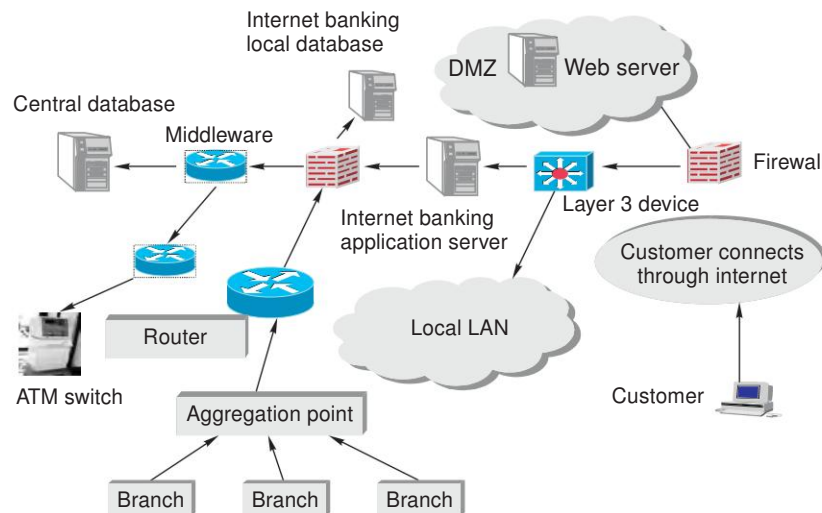


Fig. 10.2 CBS functional setup, with three tiers, Internet banking and ATM switch

The external dependencies, of the above infrastructure, are as follows:

- The network service provider,
- The Internet Service Provider (ISP),
- Provider of power/electricity,
- The CUG network
- Cash in the replenishing agency case of ATM,
- Other outsourced vendors.

The external dependencies are important for two reasons, viz.:

- In case of a disaster, we have to depend on external agencies to make our disaster site, live,
- In case of a disaster in the external agencies' systems/locations, we should have alternative ways to run our business.

Now, after the network and application infrastructure/architecture and the external dependencies have been understood, we should analyze, different disaster scenarios and their effects on the business, and give a risk ranking, to the system.

CORE BANKING SOLUTION

Disaster Scenario 1: The Centralized Database is Down

In case the centralized database is down, the operation of the branches, connected to the CBS, will come to a standstill, unless, there is a branch database server, where the transactions are committed, before going to the centralized database. Although some applications provide such kind of an architecture, the throughput of the transaction, will be slower in such scenarios. In any case, the maximum amount of outage tolerance for such a scenario, can be a maximum of 1 to 2 hours and the risk ranking assigned to it is 5 (five).

The strategy selections for the above situation, are as follows:

- The bank should have a proper backup procedure, for storing the data backup in external media, preferably on tapes and also on hard disks,
- Hot backup of the database, should be taken at hourly intervals, between central BOD (beginning of day) and central EOD (End of day),
- The cold backup should be taken, once a day, after EOD,
- The backup should be stored in an offsite location, with appropriate controls,
- There should be a stand-in-database server, with the same configuration as the primary server, where the data can be replicated from the primary database server, at hourly intervals,
- The backup arrangement for the stand-in server, should be the same as in the case of the primary server,
- At least once in two months, for a week, there should be an interchange between the primary database server and the stand-in database server,
- There should be redundant components in both, the database server and the stand-in server.

Disaster Scenario 2: The Link Between the Branch and Aggregation Point, is Down

In such a case, the effect is like that in case of scenario 1, i.e. the branch operation will come to a standstill, unless there is a branch database. The maximum amount of outage for such a scenario, should therefore, be the same, i.e. maximum of 1 to 2 hours and the risk ranking assigned to it is 5 (five).

The strategy selections for the above situation, are as follows:

- There should be a redundant link, from the branch to the aggregation point,
- It should be ensured that both the links do not have the same point of failure, i.e. if both the links are from the same exchange, then the failure of the exchange, would make both the links inoperative.

Disaster Scenario 3: The Link Between the Aggregation Point and the Data Center, is Down

In such kind of a scenario, the effect will be the same, as in the case of scenario 1 and 2 and therefore, the maximum outage will be 1 to 2 hours and risk ranking is 5 (five).

- The recovery strategy for the above situation, is as follows:
- Redundant link from the aggregation point to the data center,
- Both the links should not have, a single point of failure.

Disaster Scenario 4: The Router at the Aggregation Point Fails

In this case, although the effects will be the same, as in the above cases, the recovery strategy selections, will differ. The possible strategies are as follows:

- Having a separate, stand-in router, with the same configuration, at the aggregation points.

Disaster Scenario 5: The Aggregation Point Fails

In such a situation, the effect will be the same, as in the above cases. The recovery strategy for such a scenario are as follows:

- Redundancy, at the aggregation point, at the network topology.
- Enabling routing protocols, in the routers.

Disaster Scenario 6: The Data Center Fails

The effects for such kinds of a disaster are very severe and will have the maximum effect on the business of the bank. The possible recovery strategies, for such a scenario, are as follows:

- Move to the hot site,
- Load the backup, in the hot site,
- Enable alternative routing,

The above discussions, on the possible disaster scenarios, are just some examples. Either one, or more than one of the above disaster scenarios can happen together, or a totally unexpected disaster scenario could also materialize. The BIA methodology is used, to evaluate a disaster scenario, assign it a risk ranking and decide about the alternative strategies.

INTERNET BANKING

Disaster Scenario 1: The Web Server Fails

The web server can fail for different reasons, depending on the type of hosting and configuration of the server and host (operating system). Some of the possible reasons for the failure of the web server, are as follows:

- Bug in the web server software,
- Bug in the web host,
- Attack on the server like, Denial of Services (DOS),
- Failure of the ISP, hosting the web server,
- Disaster at the bank's data center,

Although the recovery strategies will differ from one case to another, some of the important strategies to deal with the failure of the web server, are as follows:

- Having a stand-in web server, with the same IP address and synchronizing this, with the primary server, with patch updates, etc.,
- In case it is hosted at the ISP's site it should be ensured that they have alternative sites, to launch the services, in case their primary site is down,

- In any case, if the web server fails, the Internet banking services will come to a stand still. So, the maximum outage for such scenarios could be 2 to 3 hours and the risk ranking is 5.

Disaster Scenario 2: The Internet Link Fails

The reasons for the failure of the link to the Internet could be many. Some of the known reasons, are as below:

- The failure of the ISP, providing the link,
- Failure of the routers, where the links terminate.

The possible recovery strategies for such scenarios are as follows:

- Establishing redundant links from two different providers,
- Enabling load sharing, either through a load balancer or by configuring Border Gateway Protocol (BGP) at the ISP level,
- Enabling Virtual Router Redundancy Protocols (VRRP),
- In case of link failure, the Internet customers cannot access their account through the Internet. So, the maximum outage time allowed for such transactions could be a maximum of 2/3 hours and the risk ranking of the system will be 5.

Disaster Scenario 3: Components Failure

The delivery of Internet banking services, will be affected, in the case of the failure of various components of Internet banking. The risks and controls, associated with various components of Internet banking have already been discussed, in the chapter titled "Internet banking".

ATM OPERATION

Disaster Scenario 1: The ATM Switch Fail

The failure in the ATM switch can be due to, either the hardware or system software or the application software. In any case, the failure of the switch, will affect the ATM operation. The various controls that are necessary, in case of any eventualities, are as follows:

- Built-in redundancy in the hardware and system software, on which the ATM switch software operates,
- Stand-in switch, with all configurations, to be used in case of disaster.

Disaster Scenario 2: Failure in all Other, Related Components

The ATM operation will be affected in case of failure of related components, viz.

- The link failure from ATM to ATM switch,
- Failure of the core database or an other, related database, which redresses the queries related to ATM transaction,
- Failure of cash replenishment,
- Natural disaster at data center,
- Natural disaster at branches, connected to ATM,
- Results of the BIA,

The appropriate architecture of the primary site and the DR site, after taking care of the necessary redundancies mentioned above, given in Table 10.4.

Table 10.4 Disaster Scenario

<i>Business process and interdependencies</i>	<i>Outage tolerance</i>	<i>Criticality</i>
Core banking solution		5
Central database	1–2 hours	
Link failure between branch and aggregation point	2–3 hours	
Link failure between aggregation point and data center	2–3 hours	
Disaster at aggregation point	2 hours	
Disaster at data center	4 hours	
Internet banking		5
Web server	1–2 hours	
Link failure	2–3 hours	5
Components failure	1–2 hours	
ATM operation		5
ATM switch	2 hours	
Link failure	2–3 hours	
Components failure	1–2 hours	

AUDITING THE BCP-DRP

The objectives, of auditing BCP/DRP are, to verify that the Disaster Recovery Plan is adequately equipped to ensure resumption of activities of computer systems, in a timely manner, during adverse circumstances, in line with the current business continuation plan, and to reflect the current business operating environment. The various documents that needs to be collected by the auditor for this purpose are:

- Copy of the organization's Disaster Recovery Plan,
- List of implementation team members' list,
- Current copy of the organization chart,
- Current inventory,
- Copy of agreements relating to use of backup facilities.

Some of the important aspects which the auditor should asses, during the review are as follows:

- The adequacy of the plan in comparison with industry standards,
- The conformance of the plan with the prevailing standards, regulatory stipulations and/or government regulations,
- The effectiveness of the plan, by reviewing the results, from the tests carried out,
- The conformance of the recovery site with the security and environmental controls,
- The ability of personnel to react and respond quickly, in situations of disaster,

These are just some of the objectives that an IS auditor can set for himself/herself. To this end, the IS auditor needs to follow some procedures. Some of the common procedures that can be followed are:

- Obtain a current plan document and from the distributed documents, verify the date, to check the status, i.e. whether the distributed document is the current document or not,
- Determine the priorities and support for critical activities,
- Determine the accuracy of the BIA, to identify and assess mission critical activities,
- Determine whether version control and compatibility have been addressed at the recovery site,

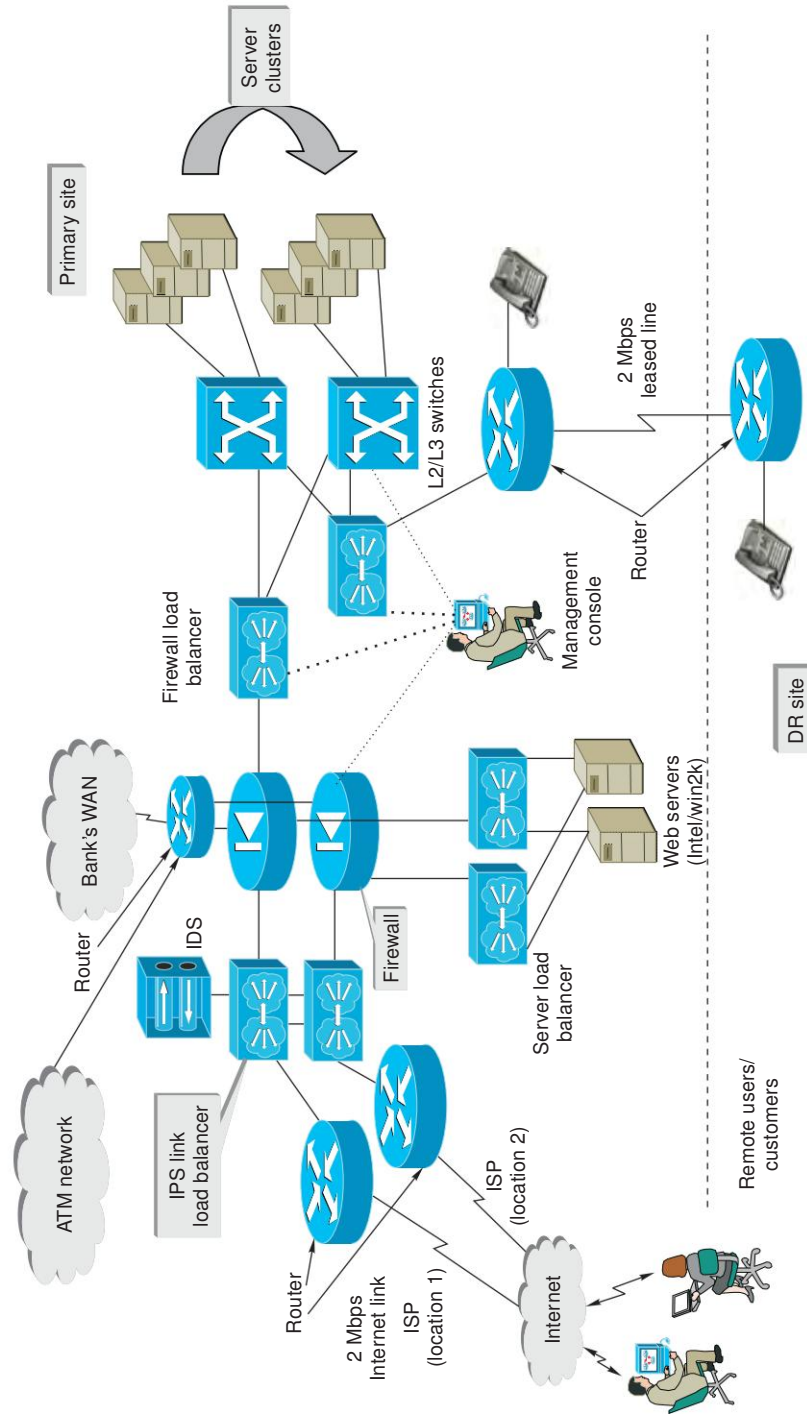


Fig. 10.3 Detailed data center network

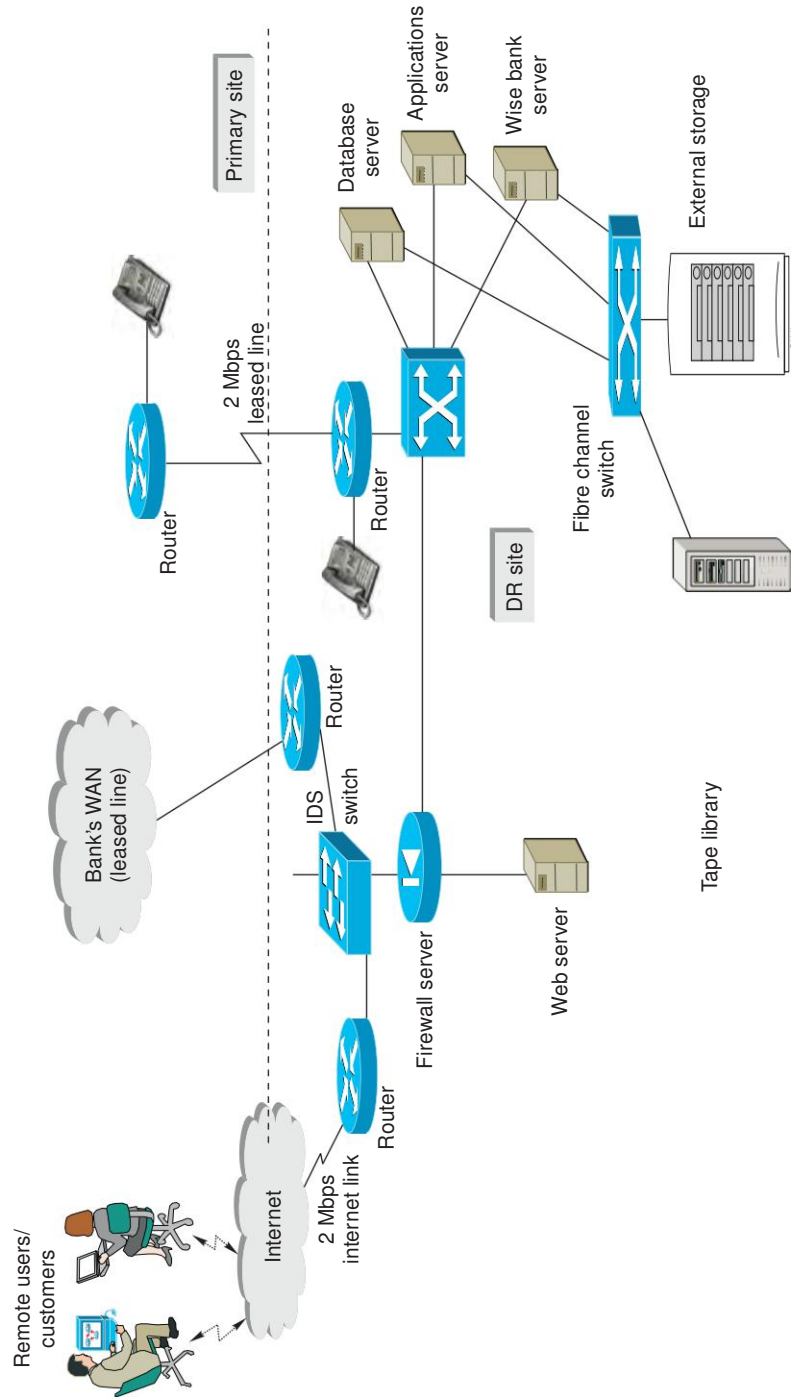


Fig. 10.4 Detailed DR network

- Verify the accuracy of the contact information, provided through a cross-checking of some randomly selected personnel, who are key players in the BCP,
- Verify the testing conditions, by simulating a disaster conditions,
- Verify the documentation done, during the testing,
- Verify the handling of the data used/generated, during the testing phase,
- Sample the procedures for easy understandability,
- Evaluate the revision and maintenance procedures.

Audit Checklist

Table 10.5

Score No =1, Not clear = 2, Clear = 3

S.No.	Issues	1	2	3
1.	Is there any mention in the plan for the disaster management committee to meet and discuss, before declaring a disaster and initiating business continuity measures?			
2.	Is there a well-defined and approved planning process framework?			
3.	Is the planning process, primarily concerned with the mission critical activities, dependencies and single points of failure?			
4.	Does the BCP, identify and comply with the prevailing legal and regulatory requirements?			
5.	Does the BCP, reflect the industry standard good practices?			
6.	Are insurance issues clearly addressed in the plan?			
7.	Is the planning process integrated (i.e. does it cover the organization's geographical presence, by taking all the sites and various factors associated with those sites, into consideration)?			
8.	Are organizational roles and responsibilities clearly understood by the personnel concerned?			
9.	Are the documented procedures sufficient for successful recovery?			
10.	Are professionally-qualified BCP-DRP practitioners involved in the planning process?			
11.	Are procedures to incorporate the feedback, given during trials and testing in place?			

(Contd)

532 *Information System Audit and Assurance*

S.No.	Issues	1	2	3
12.	Is there any grading system to address disasters of varying degrees?			
13.	Are backups (data networks and voice networks) addressed?			
14.	Does the plan address loading data, processed manually, into an automated system?			
15.	Is offsite storage used to store backups of vital information, required for processing operations?			
16.	Does the BCP reflect the current BIA?			
17.	Does the BCP identify the owner of the plan document and define the responsibilities thereof?			
18.	Is the plan document marked confidential and is it kept secured?			
19.	Is there a non-disclosure clause in the BCP, which is applicable to participating, third parties and vendors, as well as to those personnel, involved in the exercise?			
20.	Has the legal department been involved in the planning stage?			
21.	Are the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), well-defined in the plan?			
22.	Are the review and audit procedures in the plan, well-defined and scheduled periodically?			
23.	Does the plan have a section on quick reference and easy-to-use, step-by-step guide to the usage of the document?			
24.	Is the plan presented in an organized and structured manner?			
25.	Is there any representation of the BCP management committee hierarchy?			
26.	Is there a clear distinction between emergency response (fire, flood, etc.) and BCP emergency response, recovery and restoration?			
27.	Does the plan document have a complete list of personnel (along with their current addresses and contact numbers), involved with and responsible for taking actions?			
28.	Are there clear instructions, mentioned in the plan document, to keep a copy of the document, at a secure, off-site location, apart from keeping the original, on-site?			
29.	Is the distribution of the copies of the plan document, controlled?			
30.	Are emergency evacuation-response procedures clearly highlighted, easy to locate and easy to understand?			

(Contd)

S.No.	Issues	1	2	3
31.	Is there a proper mention of the training schedule, to be imparted to those who will be involved in operations?			
32.	Are the lists of emergency services, suppliers, vendors and others, who may be involved in the restoration process, clearly mentioned?			
33.	Are there procedures, in place, that can challenge and review the assumptions, if any, upon which the BCP strategy is based?			
34.	Does the BCP address both, technical and non-technical issues?			
35.	Is the BCP aligned with the overall objective and mission of the organization?			
35.	Are the critical success factors defined in the plan?			
37.	Have the risks, associated with each BCP strategy alternative, been assessed against the BIA?			
38.	Has the cost-benefit analysis of the various BCP alternatives, been prepared and presented to the senior management?			
39.	Is the strategy for dealing with the media, a part of the plan?			
40.	Is the implementation and maintenance of the BCP, closely and strictly, monitored and evaluated?			
41.	Are BCP roles and responsibilities clearly defined, within the overall job responsibilities, at each and every level of the organization?			
42.	Is the BCP integrated with the organization's performance management and appraisal system?			
43.	Does the BCP contain clearly defined and documented Key Performance Indicators (KPI)?			
44.	Is the BCP an integral part of the organization's change management and project management process?			
45.	Is there a properly defined Management Information System (MIS), to monitor and evaluate the BCP competency of the staff?			
46.	Is the internal training program for BCP, well-defined?			
47.	Does the budgetary allocation include, training to the personnel?			
48.	Apart from training to the key personnel, are there concrete plans to ensure an overall awareness among all the staff members of the organization?			
49.	Are there formal training and professional development plans for key personnel, involved in the BCP?			

(Contd)

534 *Information System Audit and Assurance*

S.No.	Issues	1	2	3
50.	Does the BCP audit program focus on the organization's mission critical activities, their dependencies and single points of failure?			
51.	Does the audit program, provide a documented, scheduled audit cycle?			
52.	Does the BCP audit contract, define the audit framework and process?			
53.	Is the scope of the audit, defined in the plan?			
54.	Does the scope of the audit, indicate the department/ work area of the organization, to be audited?			
55.	Is there prioritization of the departments, to be audited?			
56.	Does the audit contract, clearly identify any external or professional assistance, required to perform the audit?			

The following scores are only indicative and do not reflect any inherent importance of the points, listed in the preceding checklist. On conducting an audit, on the BCP of an organization, and scoring, the scores resultant reveal the following:

- **If the score is equal to or less than 60:** This organization either does not have a BCP-DRP worth its name, or the BCP-DRP has been prepared in order to fulfil some regulatory requirement.
- **If the score is between 61 and 100 (both inclusive):** Though this organization has a BCP-DRP, there are a lot many points that are not clearly defined/ understood/ documented and the plan needs to be vastly improved.
- **If the score is between 101 and 140 (both inclusive):** This organization has quite a well-defined BCP-DRP. Yet there are areas wherein, it can afford improvement.
- **If the score is greater than 140:** This organization has a very well-defined BCP-DRP. It needs to maintain, test and review its plan regularly, and incorporate the feedback into the plan, to keep it up-to-date, in all respects.

SUMMARY

In this chapter, we first started with a brief introduction to what a disaster is, which we all have faced and grappled with, at certain points of time in our lives. We then discussed, the need for disaster recovery planning in an

Information System. As disasters themselves, are unpredictable, the exact reasons for causal of disasters cannot be known. Therefore, we discussed the various reasons that could result in disastrous conditions, viz. natural calamities, equipment failures, human errors, etc. After a brief discussion on the reasons, we deliberated on the differences between BCP (Business Continuity Plan) and DRP (Disaster Recovery Plan).

While BCP is more of a preventive control, DRP is essentially, a corrective control for the organization. The BCP process, which is a sort of lifecycle, starting from Business Impact Analysis (BIA), to testing and maintaining the plan, was discussed in detail. In case of Business Impact Analysis, we also considered the different approaches to BIA like, assessment of questionnaires, checklists, interviews and BIA the matrix. The logical step after BIA, is to decide on the correct recovery strategies, based on criticality of the system, cost, time required to recover, and security. The recovery strategies include, setting up of a cold site, warm site, duplicate information processing facility or reciprocal agreement. The control issues related to these alternatives, were discussed.

After this, we went on to see, how to develop a detailed plan, wherein we deliberated on issues ranging from pre-disaster preparedness, to post-recovery options and resumption of normal operations. After discussing each step in the BCP lifecycle, we thought it useful for the readers to know, some thing about data backup and data storage techniques and accordingly different backup techniques, technology, related to storage, data replication, etc. were discussed in detail.

After this we took up the case study of a target bank, which has implemented a core banking solution, in a centralized environment. In this case, all other delivery channels, viz. Internet banking, ATM are also operational. The centralized server, Internet banking web servers and the ATM switch, are located in the bank's data center, at location "X". The bank has got its own Wide Area Network, with inter-city links, connecting 25 cities across the country. For prescribing a suitable disaster recovery strategy for this bank, we did a complete Business Impact Analysis and discussed the possible business impact due to failure of individual components, and finally devised an appropriate recovery strategy. This example will give the readers a practical view of devising a suitable recovery strategy, for an IT-enabled business process. After discussing the various controls, related to business continuity and disaster recovery, as usual, we gave a brief overview of the tasks that the IT auditors should perform, in reviewing the BCP/DR strategy of the organization. A generic checklist was given at the end of the chapter, which will help the auditors in consolidating their thoughts.

REVIEW QUESTIONS

1. What is the need for business continuity and disaster recovery planning, in an organization?
2. Describe in brief what you mean by 'disaster' in the Information System.
3. What are the causes, which can result in a disaster condition?
4. Describe the differences between BCP and DRP.
5. What is a BCP process? Describe the lifecycle of a Business Continuity Plan.
6. What is Business Impact Analysis (BIA)? Describe the different approaches to BIA.
7. Describe the different types of recovery strategies and the criteria for their selection.
8. Describe the various issues and factors, involved in recovering from a disaster, ranging from pre-disaster preparedness, to post-recovery operation and resumption of normal operations.
9. Describe the various types of tests required for BCP/DR.
10. Describe the different types of data storage technologies.

MULTIPLE CHOICE QUESTIONS

1. Which of the following is the most likely objective of the organization, in having a Business Continuity Plan?
 - (a) To facilitate the business to maintain its operations, in the event of any disaster.
 - (b) To facilitate the organization, to continue their operations, in case of disruption to Information System infrastructure or any of its components.
 - (c) To protect the organization from sustaining any reputation loss, in case of a disaster.
 - (d) To minimize the loss, in case of a disaster.
2. Which of the following would warranty a quick continuity of operations, when the recovery time window is short?
 - (a) A duplicate information processing facility.
 - (b) Duplicated data, in a remote site.
 - (c) A manual contingency procedure.
 - (d) Transfer of data, the moment a contingency occurs.

3. An offsite backup facility, having electrical writing, air-conditioning, flooring, etc., but no computer or communications equipment, intended to operate an information processing facility, is better known as a:
 - (a) Cold site.
 - (b) Warm site.
 - (c) Duplicate processing facility.
 - (d) Dialup site.
4. All of the following are security and control concerns, associated with disaster recovery procedures, except:
 - (a) Loss of audit trail.
 - (b) Insufficient documentation of procedures.
 - (c) Inability to resolve system deadlock.
 - (d) Inability to restart under control.
5. Which of the following is an important consideration, in providing backup for online systems?
 - (a) Maintaining system software parameters.
 - (b) Ensuring periodic dumps of transaction logs.
 - (c) Ensuring grandfather-father-son file backups.
 - (d) Maintaining important data, at an offsite location.
6. A large chain of shops, with Electronic Funds Transfer (EFT), at point-of-sale devices, has a central communications processor for connecting with the banking network. Which of the following is the BEST disaster recovery plan for the communications processor?
 - (a) Offsite storage of daily backups.
 - (b) Alternative standby processor, onsite.
 - (c) Installation of duplex communication links.
 - (d) Alternative standby processor, at another network node.
7. Which of the following would an IS auditor consider to be the MOST important to review, when conducting a business continuity audit?
 - (a) A hot site is contracted for and available, as needed.
 - (b) A business continuity manual is available and current.
 - (c) Insurance coverage is adequate and premiums are current.
 - (d) Media backups are performed on a timely basis, and stored offsite.
8. An IS auditor, performing a review of the backup processing facilities, would be MOST concerned that:
 - (a) Adequate fire insurance exists.
 - (b) Regular hardware maintenance is performed.

- (c) Offsite storage of transaction and master files exists.
 - (d) Backup processing facilities are fully tested.
9. Which of the following is a continuity plan test, that uses actual resources to simulate a system crash, to cost-effectively obtain evidence about the plan's effectiveness?
- (a) Paper test.
 - (b) Post test.
 - (c) Preparedness test.
 - (d) Walkthrough.
10. While reviewing the Business Continuity Plan of an organization, the IS auditor observed that the organization's data and software files are backed up, on a periodic basis. Which characteristic of an effective plan, does this demonstrate?
- (a) Deterrence.
 - (b) Mitigation.
 - (c) Recovery.
 - (d) Response.
11. During an audit of a reciprocal disaster recovery agreement, between two companies, the IS auditor would be PRIMARILY concerned about:
- (a) The soundness of the impact analysis.
 - (b) Hardware and software compatibility.
 - (c) Differences in IS policies and procedures.
 - (d) Frequency of system testing.
12. An IS auditor discovers that an organization's Business Continuity Plan provides for an alternative processing site, that will accommodate fifty percent of the primary processing capability. Based on this, which of the following actions should the IS auditor take?
- (a) Do nothing, because generally, less than twenty five per cent of all processing is critical to an organization's survival, and the backup capacity therefore is adequate.
 - (b) Identify applications that could be processed at the alternative site and develop manual procedures, to backup other processing.
 - (c) Ensure that critical applications have been identified and that the alternative site could process all such applications.
 - (d) Recommend that the information processing facility, arrange for an alternative processing site, with the capacity to handle at least seventy five per cent of normal processing.

13. An IS auditor, reviewing the results of a test of the Disaster Recovery Plan, conducted at a warm site, notes that clients were unable to logon to the restored online systems, as there were insufficient data lines connecting the client premises to the recovery site. The MOST likely conclusion drawn by the IS auditor would be that the:
 - (a) Clients were not involved sufficiently, in the development of the plan.
 - (b) Use of a warm site is inappropriate.
 - (c) Impact of a potential disaster was not fully analyzed.
 - (d) External communications service providers, were not involved in the test.
14. Which of the following methods would BEST ensure the adequacy of a Disaster Recovery Plan?
 - (a) Regular reviews of the timeliness of information, detailed in the plan.
 - (b) Unannounced shut down of the primary installation, during quiet periods.
 - (c) Regular recovery exercises, using expert personnel.
 - (d) Unannounced recovery exercises, at regular intervals.
15. Which of the following is a risk, if system backups are performed only weekly?
 - (a) System defaults are inaccurate.
 - (b) System files are not synchronized with data access.
 - (c) System files are partially fragmented.
 - (d) System defaults are lost.
16. Classification of Information Systems is essential in Business Continuity Planning. Which of the following system types cannot be replaced by manual methods?
 - (a) Critical system.
 - (b) Vital system.
 - (c) Sensitive system.
 - (d) Non-critical system.
17. An IS auditor should be involved in:
 - (a) Observing tests of the Disaster Recovery Plan.
 - (b) Developing the Disaster Recovery Plan.
 - (c) Maintaining the Disaster Recovery Plan.
 - (d) Reviewing the disaster recovery requirements of supplier contracts.

18. The window of time recovery, of information processing capabilities, is based on the:
 - (a) Criticality of the processes affected.
 - (b) Quality of the data to be processed.
 - (c) Nature of the disaster.
 - (d) Applications that are mainframe-based.
19. During an IT audit of a large bank, you observe that no formal risk assessment exercise has been carried out for the various business applications, to arrive at their relative importance and recovery time requirements. The risk that the bank is exposed to, is that the:
 - (a) Business Continuity Plan may not have been calibrated to the relative risk, that the disruption of each application poses, to the organization.
 - (b) Business Continuity Plan may not include all relevant applications and therefore, may lack completeness, in terms of its coverage.
 - (c) Business impact of a disaster may not have been accurately understood by the management.
 - (d) Business Continuity Plan may lack effective ownership, by the business owners of such applications.
20. During a Business Impact Analysis, which of the following questions should be asked FIRST?
 - (a) What are the organization's critical information resources?
 - (b) Who is the organization's critical information system staff?
 - (c) What is the organization's critical recovery time period?
 - (d) What is the organization's critical system?

DISCUSSIONS AND RESEARCH QUESTIONS

1. Business continuity planning is more of a preventive control, than the Disaster Recovery Plan, which is a corrective control. Discuss this statement, in the context of the distinction between BCP and DRP.
2. If disaster is unpredictable, then how do we know the reasons for disaster and take preventive action? Discuss in the context of the causes for conditions of disaster.
3. Discuss the differences between Recovery Time Objective (RTO) and Recovery Point Objective (RPO), with the help of examples.
4. Development of effective questionnaires, is the key to adopting the questionnaire analysis approach, for conducting Business Impact Analysis (BIA). Discuss.

5. Describe the flip side of a Duplicate Information Processing facility.
6. Describe the various controls required, for entering into a reciprocal arrangement for managing disaster, in an organization.
7. BCP is more a business concern, than solely a technology concern. Discuss in the context of planning business continuity.

EXERCISES

1. Describe the various steps required, to conduct a BIA, in a bank, which has implemented a core banking solution.
2. Devise a simple checklist for auditing DRP, for Internet banking.
3. A research and development organization, viz. Banksearch, is involved in various activities including, providing network bandwidth to the banking community, providing other services like, mail messaging services, web hosting, etc. The services wing and the R&D wing of the organization, are in one Local Area Network (LAN), with a logical partition. The organization is considering formulation of BCP and DRP for the R&D wing and is in the process of consolidation of the backup.

At present, all the users in the network are logging into an authentication server which is a Windows 2000 domain controller and saving their data, in a network folder. There is also a mail-messaging server, which caters to the need of the mailing facility for the users, both inside and also to and from the Internet. There is also an ERP of the organization, which works through the organization's intranet portal. This ERP, works on a backend DBMS. Now, the CEO of the organization, has asked the internal IS audit department, to devise a suitable backup strategy for the enterprise, which does not include the services wing. You are the head of IT audit. Write a suitable note, on what needs to be backedup and what should be the periodicity, whether you need a SAN or a NAS, whether you need automation of the backup or not?, etc.
4. Write the various components of Internet banking in a centralized environment and discuss the disaster scenario, in case of failure of each component.
5. A Close User Group (CUG)'s network, "webnet" is managed by a third-party, viz. "ABC Enterprise". The members of the groups, are banks and financial institutions. The eligibility to become a member of CUG, is decided by the central bank of the country, from time to time. An electronic fund transfer application is running in this network and is used by all the users/members. The clearing and settlement of this

542 *Information System Audit and Assurance*

application is taken up by another organization, which is also a member of the CUG, but the organization is not a Bank (XYZ corporation). Now, XYZ corporation (the clearing and settlement agency) and ABC Enterprise (the network provider) is considering, entering into a reciprocal arrangement, for keeping their offsite backup, with each other. You, being a part of ABC Enterprise, are asked to list the control implications of such an exercise. Prepare such a list.

Appendix A

STANDARDIZED CHECKLIST FOR CONDUCTING COMPUTER AUDIT*

1. BUSINESS STRATEGY

- 1.1 Has the business strategy been documented, have business objectives been defined, and has the role of IT been clearly spelt out in the business strategy?
- 1.2 Have Information Technology issues and opportunities been adequately assessed and reflected in the organization's strategy, both in the long-term and short-term plans.
- 1.3 Are assessments made periodically, by the bank to ensure that IT initiatives support the organizational mission and goals?
- 1.4 Have major developments in technology (hardware, software, communication, etc.) been assessed, to study their impact on the business strategy, and have necessary corrective steps, wherever needed, been taken?

2. LONG-TERM IT STRATEGY

- 2.1 Does a long-term IT strategy exist and is it documented?
- 2.2 Does the long-term plan cover:
 - Existing and proposed hardware and networking architecture for the bank, and its rationale

- Broad strategy for procurement of hardware, software solutions, vendor development, and management
 - Standards for hardware/software, prescribed by the proposed architecture
 - Strategy for outsourcing, insourcing, procuring off-the-shelf software, and in-house development
 - Information security architecture
 - IT department's organizational structure
 - Desired level of IT expertise in bank's human resources and plans to bridge the gaps, if any
 - Strategies converted into clear IT initiatives, with a broad timeframe
 - IT costs and cost management
 - Plan for transition, if any
- 2.3 Has the long-term plan been approved by the board?
- 2.4 Has the organization structure of IT been made part of the IT plan?
- 2.5 Does the IT long-range plan support the achievement of the organization's overall mission and goals?
- 2.6 Has a structured approach to the long-range planning process been established?
- 2.7 Does the plan cover the what, who, how, when, and why of IT?
- 2.8 Prior to developing or changing the long-term Information Technology plan, did the management of the information services function assess the existing Information Systems, particularly the degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses, etc., to determine the degree to which the existing systems, support the organization's business requirements?
- 2.9 At the time of planning, were factors like, organizational model and changes to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third-parties or the market, planning horizon, business process re-engineering, staffing, in or outsourcing, etc. taken into account?
- 2.10 Does the plan refers to other plans such as, the organizational plan and the information risk management plan?
- 2.11 Does the process provide for timely and accurate modification of the long-range IT plan, taking into account the changes in the organization's plan and also in business and Information Technology conditions?

- 2.12 Has a security committee, comprising of senior functionaries from the IT department, business group, IT security department, and the legal department been formed, to provide appropriate direction for formulation, implementation, monitoring and maintenance of IT security in the entire organization?

3. SHORT-RANGE IT PLANS

- 3.1 Are long-range IT plans converted to short-range IT plans, regularly, for easy achievability?
- 3.2 Does the IT short-range plan cover the following?
- Plan for initiatives, specified in the long-range plan or initiatives that support the long-range plans
 - System-wise transition strategy
 - Responsibility and plan for achievement
- 3.3 Have adequate resources been allocated, for realizing the short-range plans?
- 3.4 Are short-range plans amended and changed periodically, as necessary, in response to changing, business and Information Technology conditions?
- 3.5 Are assessments made on a continuous basis of the implementation of short-range plans?
- 3.6 Have clear-cut responsibilities been fixed, for realizing the short-range IT plan?

4. IS SECURITY POLICY

- 4.1 Is a well-documented security policy is available?
- 4.2 Has the inventory of IT assets been made part of the policy? Is the inventory of IT assets kept at the branch/office level?
- 4.3 Are policies related to IT activities, listed in the security policy?
- 4.4 Does the policy take into account, the business strategy/plan for the next 3 to 5 years?
- 4.5 Does the policy take into account, the legal requirements?
- 4.6 Does the policy take into account, the regulatory requirements?
- 4.7 Has the policy been approved and adopted by the board of directors/top-management?

546 *Information System Audit and Assurance*

- 4.8 Has the policy been communicated to all concerned and is it understood by them?
- 4.9 Are the following major security areas covered in the policy?
 - PC and LAN, MAN and WAN security
 - Physical security of IS establishments
 - Handling of confidential information
 - Handling of security incidents
 - Privacy-related issues, for outside entities
 - E-Mail security
 - Application security
 - Interface security
 - Password security
 - Operating system security, website security
 - Database security
 - Antivirus and piracy policy
 - Archived and backup data security
 - Procedures for handling incidences of security breach
 - Disaster Recovery Plan
 - Use of cryptology and related security
 - Persons responsible for implementing security policy and consequence of willful violation of the security policy
- 4.10 Is a review process, in place, for reviewing the policy at periodic intervals and/or on any other important occasion?

5. IMPLEMENTATION OF SECURITY POLICY

- 5.1 Has the documented security policy been made available to all levels of users, to the extent, relevant to them?
- 5.2 Are continuous awareness programmes conducted for security awareness?
- 5.3 Has the Information Security Officer been assigned responsibilities for implementation of the security policy?
- 5.4 Have detailed procedures for each policy statement been developed?
- 5.5 Have suitable methodologies been adopted for implementation?
- 5.6 Have suitable security tools been selected for implementation?

- 5.7 Are the roles of those, in charge of implementing the policy, clearly defined?
- 5.8 Has the budgetary allocation for implementation of the IS security policy been assessed and documented?
- 5.9 Are periodic security audits carried out?
- 5.10 On the basis of audit reports or any other vital information, are suggestions for updating the security policies conveyed to the right/appropriate level of management?
- 5.11 Does the management demonstrate adherence to the security policy?
- 5.12 Are new entrants given adequate exposure to the security policy?
- 5.13 In cases of breaches in security policy, is the root cause analysed and preventive and corrective action taken?
- 5.14 Have incidence-reporting procedures been followed?
- 5.15 Has the Information Security Officer been assigned the tasks of reporting instances of non-compliance with the approved policy and also incidents of security breaches, to the top-level management, and to initiate and effect corrective action?

6. IS AUDIT GUIDELINES

- 6.1 Are a documented and approved IS Audit guidelines available?
- 6.2 Are the IS Audit guidelines consistent with the security policy?
- 6.3 Have the IS Audit responsibilities have been assigned to a separate unit, which is independent of the IT department?
- 6.4 Is periodic, external IS Audit carried out?
- 6.5 Is independent security audit conducted, periodically?
- 6.6 Have contingency planning, insurance of assets, data integrity, etc. been made part of external audit?
- 6.7 Have vulnerability and penetration testing been made part of external audit?
- 6.8 Have the major concerns, highlighted by previous audit reports been brought to the notice of the top-management?
- 6.9 Has necessary corrective action been taken, to the satisfaction of the management?
- 6.10 Are adequate training facilities provided to IS Audit teams, to enable them to conduct audits effectively?
- 6.11 Is the IS Audit team encouraged to keep itself abreast of the latest developments?

- 6.12 Do IS auditors exchange their views and share their experiences within the organization?

7. ACQUISITION AND IMPLEMENTATION OF PACKAGED SOFTWARE

The process of procurement and implementation of packaged software has various stages. The Information System auditor (SA) has to familiarize him/herself with the policies and practices of the bank, with regard to software procurement and implementation. The IS auditor should have prior discussions with the IT department to gain knowledge of the following before commencing audit work in this area:

- IT infrastructure and environment in the bank,
- Resources available in the IT department of the bank,
- Software products procured and implemented during the period,
- Status of the implementation,
- Problems, if any, faced by the users after implementation,
- Errors noticed in processing transactions, in the procured system,
- Any errors, resulting in financial loss, regulatory/ compliance issues, serious customer complaints, etc.

Note: This checklist does not address commercial considerations, for which regular audit guidelines have to be used.

This checklist is divided into the following areas:

- (a) Requirement identification and analysis
- (b) Product and vendor selection criteria
- (c) Vendor selection process
- (d) Contracting
- (e) Implementation
- (f) Post-implementation issues

(a) Requirement Identification and Analysis

- 7.1 Is there an annual plan, covering areas, requiring computerization, approved by the top-level management?
- 7.2 Is the plan in line with the bank's overall IS strategy?
- 7.3 Has a functional manager or committee been identified, as responsible a sponsor for an area, requiring computerization?

- 7.4 Have the costs of computerization been budgeted and included in the overall IT budget of the bank?
- 7.5 Has a detailed plan been made by the IT department, clearly mentioning the date of commencement, activities involved, target date of final implementation, and estimated costs for each area identified?
- 7.6 Has this plan been approved by the sponsor?
- 7.7 Has a document been prepared, clearly detailing the following requirements:
 - Functionality
 - In case of replacement, the problems faced in the existing system and need for replacement
 - Performance
 - Security
 - Operations risk mitigation
 - Acceptance criteria for the system
 - Changes in the operating procedures, required to implement the proposed system and persons responsible and plan for effecting the changes
 - Smooth transition/migration from the existing to the proposed plan
 - Interface requirement with other computer systems
- 7.8 Have the requirements been graded as vital, essential and desirable?
- 7.9 Has the sponsor approved the requirement document?

(b) Vendor Selection Criteria

- 7.10 Has the 'requirements document' been clearly translated into product acceptance criteria?
 - Has acceptance criteria been classified into:
 - Show stoppers
 - Allowable customizations
 - Desirable positive features
- 7.11 Does the IT department have a technology standard for product selection?

7.12 Does the technology standard cover:

- Architecture
- Open database standards
- Interfaces and API standards
- Security standards

7.13 Are the product selection criteria consistent with the IT platform of the bank? Does the bank have clearly laid-down and approved guidelines for selection of product vendors?

7.14 Do the vendor selection guidelines address the following:

- Market presence
- Years in operation
- Technology alliances
- Desired size
- Customer base and existing implementation
- Support
- Possibilities of partnership or strategic alliance
- Source code availability
- Local support, in case of foreign vendors

7.15 Has the selection criteria been decided by the IT department, in consultation with the user departments?

7.16 Has the sponsor approved the selection criteria?

7.17 Does the policy of the bank permit beta-site installations? If yes, are criteria for selection, distinctly different from regular guidelines?

7.18 Does the IT department use the scoring model for evaluating the products and vendors?

7.19 Do the scoring criteria, consider the following factors:

Extent of customization and work-around solutions

- Security features
- Technology fit
- Performance and scalability
- Number of installations
- Existing customer reference
- Cost
- Vendor standing

(c) Vendor Selection Process

- 7.20 Does the IT department have a system to identify potential vendors for an area such as subscription to magazines, rating reports and reports of specialized agencies such as, Gartner, IDC, Data Quest, etc.?
- 7.21 Are reports of specialized, independent rating agencies used for short-listing vendors?
- 7.22 Does the bank have a system of floating formal RFP (Request for Proposal), for systems with estimated budgets, exceeding a certain amount?
- 7.23 Is there a core team, comprising of personnel from the IT Department, functional departments, and internal audit department, and in charge of vendor selection and implementation?
- 7.24 Is the process of selection for each area, approved by the sponsor?
- 7.25 Are meetings of the core team documented?
- 7.26 Does the team use prepared checklists for:
 - (a) Product evaluation
 - (b) Site visits
 - (c) Customer reference
- 7.27 Is final evaluation and selection, fully- documented and approved by the sponsor?
- 7.28 Does the document clearly reflect the rationale underlying the selection?

(d) Contracting

- 7.29 Does the bank have approved terms and conditions for product licensing agreements?
- 7.30 Do the licensing terms contain:
 - (a) Escrow mechanism for source codes
 - (b) Facilities for minor customization
 - (c) Maintenance and upgrades
- 7.31 Does the bank have a Service Level Agreement with product vendors for support and maintenance?
- 7.32 Where there is a contract with a distributor or reseller, is there a commitment to ensure that the actual owner will support the bank, in case the relationship between the owner and the reseller, breaks?

- 7.33 Does the contract clearly segregate duties and responsibilities of the bank and the vendor?
- 7.34 Does the contract include a clause to protect the bank against a Vendor using the bank data?
- 7.35 Does the contract clearly specify the product baselines?

(e) Implementation

- 7.36 Is the analysis of the gap between the requirement and the selected product, carried out and is it documented?
- 7.37 Does this document act as the basis for further implementation of plans?
- 7.38 Does the bank's policy provide for a parallel run of the previous system, during the implementation period?
- 7.39 Is there an agreed plan for implementation? Has the plan been approved by the sponsor, vendor, and IT department?
- 7.40 Does the implementation plan clearly identify product customization requirements, user acceptance criteria, and tests for such customization?
- 7.41 Does the implementation plan address the issue of data migration from previous systems?
- 7.42 Does the implementation, cover the following:
 - (a) User departments' involvement and their role
 - (b) User training
 - (c) System administration training
 - (d) Acceptance testing
 - (e) Role of vendor and period of support
 - (f) Required IT infrastructure plan
 - (g) Risk involved and actions required, to mitigate risks
- 7.43 Does the responsibility for accuracy of key parameters/static data, rest with the functional department?
- 7.44 Is there a list of areas which will be controlled by the vendor, during the implementation phase?
- 7.45 Does the bank have a test environment, to simultaneously allow familiarization during the implementation process? Have errors that have been identified during the implementation phase, been documented and has the root cause of the errors been analysed and confirmed by the software vendor?

- 7.46 If there are bugs and errors, due to design flaws, are they forwarded to higher levels in the software Vendor's organization and in the bank?
- 7.47 Are test packs developed by user groups, for testing customization, delivered by the vendor?
- 7.48 Is there a clearly identified data integration strategy for the customization period (If customization involves additional elements of data to be captured)?
- 7.49 Is the result of testing, properly documented?
- 7.50 Are necessary changes to system documents carried out, on customization?
- 7.51 Have all the following documents been handed over by the vendor?
 - System documentation covering design and program documentation
 - Data dictionary
 - Installation manual
 - User manual
 - Troubleshooting guide
- 7.52 Does the IT department have a proper archival system for these documents?
- 7.53 In cases where source code is given by the vendor, has the IT department undertaken a technical conversion and issued a confirmation of satisfactory compilation/performance?
- 7.54 Is there a system to issue a formal Acceptance Certificate, signed off by the user department, IT department, and the sponsor?

(f) Post-implementation Issues

- 7.55 Has the IT department taken the required consequential action for backup, disaster recovery, and performance tuning?
- 7.56 If source codes are delivered, are they baselined as per the IT department procedures?
- 7.57 Has the IT department, in consultation with the user department, worked out the database controls?
- 7.58 Has the IT department introduced a system to track the problems reported by users, forward these to the vendor and resolve them?
- 7.59 Is there a system of measuring the vendor's support to the agreed service levels?

- 7.60 Is there an identified system administrator, who is responsible for managing access to the system, backup, and ensuring database controls?

8. DEVELOPMENT OF SOFTWARE: IN-HOUSE AND OUTSOURCED

Audit Framework for Software, Developed In-house

Software Audit Administration

- 8.1 Is the software audit conducted, using pre-designed formats at the following three levels, viz.:
- (a) Program level,
 - (b) Application level, and
 - (c) Organization level
- 8.2 Has the IT department adopted any standardised quality processes such as, ISO, SEICMM, etc. for software development?
- 8.3 Are instances of non-compliance, reported in such quality audit exercises, properly attended to and rectified?
- 8.4 Is there a system, in place, to reveal the outcome of the audit to the staff members of the bank, at respective levels?
- 8.5 Is there a structure, in place, for effective software audit, so that reliable results can be obtained?

Software Audit Process

Audit at Program Level

- 8.6 Are the programs developed by drafting formal specifications, and defining scope, application, input data elements, output requirements, process work flow, etc.?
- 8.7 Is the software tested for quality assurance?
- 8.8 Is the quality assurance team, different from the development team?
- 8.9 Are data/ test results preserved for future reference?
- 8.10 Are there temporary patches that are developed, by simply copying a few set of legacy programs? If so, are they tested properly before deployment. Also, are the limitations and conditions, which such programs cannot handle, communicated to the users and are appropriate control procedures, put in place?

- 8.11 Do all the program source codes contain a title area, specifying the author, date of creation, last date of modification, and other relevant information?
- 8.12 Are there adequate input validation checks, built into the data entry programs?
- 8.13 Are the following manuals prepared?
 - Systems operations/ installation manual
 - User manual
- 8.14 Are there well-established testing procedures? Do the testing procedures cover:
 - Questions of what, when and how to test
 - Positive (test done, by processing valid data and checking if the results are accurate) and negative testing (tests done, by processing invalid data and checking if the program generates necessary error messages)
 - Performance and scalability
 - Recording and maintaining test results
- 8.15 Is parallel testing, at a few pilot installations, done, after completing pre-implementation testing?
- 8.16 Have programs that have been successfully implemented, passed the test for accuracy of the outputs generated?
- 8.17 Is the source code location, with ownership for future up-gradation, well-established?
- 8.18 Is every patch/update authorized by a competent authority?
- 8.19 Does development take into account security requirements, as per the approved security policy?

Audit at Application Level

- 8.20 Are operational controls such as, distinct user passwords, etc., in place and have they been enforced?
- 8.21 Have necessary 'regulatory compliance' requirements been taken into account by the user?
- 8.22 Has SRS taken into account, errors, frauds, disclosures, interruptions, organizational risks, etc.?
- 8.23 Are input/output controls in place?
- 8.24 Are validation controls, viz. field, transactions, file, in place, with appropriate error reporting?

556 *Information System Audit and Assurance*

- 8.25 Are appropriate data classifications with security, in place, viz. read only for users, read/write for authorized persons?
- 8.26 Is audit trail built into the systems?
- 8.27 Does the system provide for 'exception reporting'?
- 8.28 Have adequate firewalls been set up, to ensure that any outside access being provided, is limited in scope and does not intrude on sensitive data areas?
- 8.29 Is user acceptance recorded, along with test plan data, test data, test results, etc., for future reference?
- 8.30 Has the user signoff been obtained?

Audit at Organizational Level

- 8.31 Has an updated organizational chart been maintained?
- 8.32 Are the duties of developers and operators of the system, distinctly segregated?
- 8.33 Is job rotation, in place?
- 8.34 Has the software implementation plan been approved by the controlling authority?
- 8.35 Has a provision been made for maintenance of the software library?
- 8.36 Is there a system in place, for software distribution?
- 8.37 Are error reporting and control mechanisms, in place?
- 8.38 Is there a system for post-completion 'review audit'?
- 8.39 Is there a standard and secure procedure for up-keep of the source/object code?
- 8.40 Are security controls, including disaster recovery, in place?
- 8.41 Is the data conversion, audited?
- 8.42 Are all changeovers from one system to another, authorized by a competent authority?
- 8.43 Are the training requirements for users properly identified?
- 8.44 Is the DRP in place, at all operating offices?
- 8.45 Is documentation available, at the operational stage, to facilitate formal changeover of jobs?

Audit Framework for Software Outsourcing

- 8.46 For software development outsourcing, are there laid-down criteria for the selection of vendors?

- 8.47 Is there a formal outsourcing strategy, in place, for necessary interface with the vendor?
- 8.48 Are outsourcing activities evaluated, based on the following practices:
 - The objective behind outsourcing
 - The in-house capabilities, in performing job
 - The economic viability
 - The in-house infrastructure deficiencies and the time period involved
 - The risks and security concerns
 - The outsourcing arrangement and fallback method
 - Arrangements for obtaining the source code for the software
- 8.49 Is there a formal system, in place, for approval from the head of the user department?
- 8.50 Does the user department's representative, the 'expert officer' visit the vendor's premises for reviewing the capability and quality of software development activities?
- 8.51 Does the vendor report on the progress of software development, at periodic intervals?
- 8.52 Is there a formal, product handover and project completion system, in place?
- 8.53 Is there an agreement, entered into, by the bank with the vendor for completion of software development, in time. Does any penalty clause exist, for delayed completion of work?

9. PHYSICAL ACCESS CONTROLS

- 9.1 Is there a policy regarding physical access control and is it a part of the security policy of the organization?
- 9.2 Is there a mechanism to review the policy, regularly?
- 9.3 Does the policy address the following, appropriately:
 - Layout of facilities
 - Physical and logical security
 - Safety
 - Access
 - Maintenance
 - Signage

558 *Information System Audit and Assurance*

- Visitors
 - Health
 - Safety and environmental requirements
 - Entrance and exit procedures
 - Regulatory requirements
 - Legal requirements.
- 9.4 Is the Information System facility, located in a place, which is externally not obvious?
- 9.5 Is the facility located in an area that is least accessible or where access is limited to authorized personnel, only?
- 9.6 Are the physical access, control procedures adequate for employees, vendors, equipment, and facility-maintenance staff?
- 9.7 Are the 'key' management procedures and practices adequate? Are reviews and updates carried out, on a 'least access needed' basis?
- 9.8 Are the access and authorization policies on the following, adequate?
- Entering/leaving
 - Escort
 - Registration
 - Visitor passes
 - Surveillance cameras
- 9.9 Have the policies that have been laid down, implemented?
- 9.10 Is a periodic review of access profiles, carried out?
- 9.11 Are the revocation, response, and escalation processes in the event of a security breach, appropriate?
- 9.12 Is the security for portable and off-site devices, adequate?
- 9.13 Is the issue of control of visitors, adequately addressed? Have issues like, registration, pass, escort, logbook for checkin and checkout, been handled properly?
- 9.14 Are fire-prevention and other control measures that have been implemented, adequate and are these tested, periodically?
- 9.15 Are computing facilities situated in a building that is fire-resistant and are the wall, floor and false ceiling non-combustible?
- 9.16 Are smoking restrictions, in computing facilities, in place?
- 9.17 Are smoke/heat-rise detectors, installed and connected to the fire alarm system?

- 9.18 Have fire instructions been clearly posted and are fire alarm buttons, clearly visible? Have emergency power-off procedures been laid down and are evacuation plans, with clearly responsibilities, in place?
- 9.19 Are fire drill and training conducted, periodically?
- 9.20 Are computing facilities located above ground level? Are there measures to prevent water leakage, seepage, etc.?
- 9.21 Are air-conditioning, ventilation and humidity control procedures in place? Are these tested periodically and given adequate attention?
- 9.22 Has security awareness been created, not only in IS function domain, but also, across the organization?
- 9.23 Is physical security continually addressed? Has physical security been ensured at the supplier's facilities, especially in cases where organization's assets, either physical or data are processed at the supplier's facilities?
- 9.24 Is UPS available? If so, is it covered under maintenance?
- 9.25 Are alternative or re-routing telecommunication lines available?
- 9.26 Are alternative water, gas, air-conditioning, and humidity resources, available?
- 9.27 Have all access routes been identified and are controls, in place?
- 9.28 Is the computer room locked and is access to it restricted?
- 9.29 Does the IT staff avail holidays and vacations that are permitted to them?
- 9.30 Are hazardous commodities stored in the IS area?
- 9.31 Are appropriate access controls like, password, swipe card, biometric devices, etc., in place and do adequate controls exist, for storing data/information on them?
- 9.32 Wherever access to the IS facility is enabled through ID cards/badges, etc., are there controls to ensure that the issue and re-collection of such access devices are authorized and recorded?
- 9.33 In case of outsourced software, is all the maintenance work carried out, only in the presence of/with the knowledge of the appropriate bank staff?
- 9.34 Based on criticality of the IS facility, is there video surveillance equipment to monitor the movements of the personnel inside the facility? If so, check whether continuity of video recording is ensured.
- 9.35 Are access violations recorded and forwarded to higher authorities and is appropriate action taken.

10. OPERATING SYSTEM CONTROLS

Adherence to Licensing Requirements

- 10.1 Does the branch/office, hold the original license, from the Head Office/vendor, for using the operating system software?
- 10.2 Is the original operating system media, supplied by the vendor available in the branch/office?
- 10.3 Verify all the manuals and user guides provided by the vendor, at the time of supply of the system and ensure that all these are physically available. Ensure that proper library records are maintained by the branch/office for all the manuals/books, received along with the package.
- 10.4 Ascertain if the number of licenses, used in the branch/office, is less than or equal to the number of user licenses mentioned by CPPD/vendor in the license.

Version Maintenance and Application of Patches

- 10.5 Verify the system configuration such as memory, clock speed, hard disk size, OS version, etc. and ensure that they are, as per the order or terms, stipulated by CPPD/IT Department, at the time of procurement.
- 10.6 Ensure that the latest OS version is running at the site. Check whether latest updates/patches, released by the OS vendor, have been applied.

Network Security

- 10.7 Check if the system being audited, trusts other hosts for providing logon access to similar user accounts (same user account in the system, being audited and the host system), in both the systems, without supply of the password. If so, ensure that it has been implemented in accordance with IT/CPPD guidelines only.
- 10.8 Check if remote logon is enabled and if so, whether it is as per the guidelines of CPPD/IT department. Ensure that the users logging on from remote locations, are identifiable by terminal IDs/IP addresses.
- 10.9 Check if remote logon, through services such as, ftp, telnet, etc. is disabled. If not, ensure that the same has been implemented, as per the IT security policy of the bank.

User Account Maintenance

- 10.10 Each and every user ID in the operating system level, should have been created, only after specific approval of the branch manager/ department head, in writing, on a request form, signed by the respective user. Verify whether such approval is in place, for all the active user IDs.
- 10.11 Apart from the approved request forms, the branch/ office should be maintaining a user profile register, with details such as:
- Employee name
 - Designation
 - Employee number
 - Date of joining the branch/ office
 - User ID allotted
 - Date of creation of user ID
 - Date of deletion of user ID
 - Signature of the user
 - Initials of the DBA
 - Initials of the BM

Verify if the above-mentioned register, is maintained. All the entries in the register should be accounted for, in the list of active user IDs, obtained from the operating system.

- 10.12 Check that, with the exception of reserved user accounts, created for the internal use of the operating system, RDBMS, application system, etc., all other user accounts are uniquely identifiable by the respective user's personal name. In other words, generic user accounts, which cannot be attributed to any individual, should not be allowed to exist. Verify and comment on this.
- 10.13 Check the operating system user IDs, which have security equivalence to super user and ascertain if they are permissible, as per the CPPD/ IT department guidelines.
- 10.14 Check whether all the user IDs are protected by passwords.
- 10.15 With the exception of the super user account, check whether all default system login accounts are disabled. In other words, ensure that all default vendor accounts, shipped with the operating system, have been disabled. This should be checked after each upgrade or installation.

562 *Information System Audit and Assurance*

- 10.16 Check the list of active user groups and ensure that general users are not members of sensitive/privileged user groups, which enjoy higher privileges.

Logical Access Controls

- 10.17 Ensure that access to operating system command prompt, is disabled for general users in the branch/ office.
- 10.18 If some or more of the system administration-related activities are driven by a menu-based utility, assigned to any user ID, which is privileged, ensure that such IDs cannot be used to bypass login security and access the command prompt.
- 10.19 Ensure that the file pertaining to each user, containing login parameters, cannot be modified by the respective user.
- 10.20 Ensure that any user, other than the super user, cannot modify the system activity log file.
- 10.21 Check whether access rights to system files, application executable program files, application data files, utilities, application parameter files, system/ database configuration/ initialization files, etc. have been adequately controlled, to allow read/ write/ execute/ modify, etc., as the case may be, to authorized users on a need to know, and 'need to do' basis.
- 10.22 Obtain a list of world writable (directories/ folders, with access to every user) directories/ folders in the system and ensure that they have been set, only in accordance with the IT/ CPPD guidelines.
- 10.23 Verify the access rights settings, for the users' home directories and ensure that they are not owned by any ID, other than that of the actual user. Also, ensure that the user's home directory, cannot be accessed by any other user.

System Administration

- 10.24 Ensure that the facility to logon as super user, is restricted to the system console, for security reasons.
- 10.25 Check the password definition parameters, included in system and ensure that the minimum password length is specified, according to the IT security policy of the bank (ideally, a password should have least 6 characters).

- 10.26 Ensure that the maximum validity period of the password, is not greater than the number of days permitted by the IT security policy.
- 10.27 Check whether the parameters to control the maximum number of invalid logon attempts, have been specified properly, in the system, according to the security policy.
- 10.28 Check whether password history maintenance has been enabled in the system, to disallow same passwords from being used again and again, on a rotational basis.
- 10.29 Verify if the parameters to control the password format, have been set properly, according to the security policy of the bank.
- 10.30 Verify the parameters in the system, to control automatic logon from a remote system and ascertain if they have been set properly, according to the organization's security policy.
- 10.31 Verify the parameters in the system, to control the number of concurrent connections a user can have, simultaneously, from different terminals and ensure that it is restricted, as per the CPPD/IT department guidelines.
- 10.32 Examine the terminal inactive time, allowed to the users and verify if the time set, is in accordance with the guidelines.
- 10.33 If the minimum, password validity period is not set properly, verify the latest date of change of privileged passwords, including that of the super user and ensure that the password is not too old, in any case, not older than a month.
- 10.34 Check whether automatic logging of user activities is enabled.
- 10.35 Check for unexpected users, logged onto the system at odd times.

Maintenance of Sensitive User Accounts

- 10.36 Ascertain who the custodian of sensitive passwords for accounts such as, super user is and verify if he/she is maintaining secrecy of the password, whether he/she has preserved the password in a sealed envelope, with movement records for usage, in case of an emergency.
- 10.37 From the log file, identify the instances of use of sensitive passwords such as that of the super user and find out if records have been maintained by the branch/office, with reasons for the same. Ensure that such instances have been approved by the CPPD/ TBC group/ IT department and that the branch manager, password custodian, and DBA have signed the record.

- 10.38 From the log file, identify the instances of unsuccessful logon attempts to the super user account and check the terminal ID/IP address from which, it is happening. Check if appropriate reporting and escalation procedures are in place, for such violations.

11. APPLICATION SYSTEMS CONTROLS

The application system, before being implemented, has to be reviewed by the auditor, if various controls suggested by users are to be incorporated in the application system. The various controls, which have to be included in the system are as follows:

- Logical security
- Input controls
- Processing controls
- Output controls
- Authorization controls
- Interface controls
- Data integrity/file continuity controls

Logical Access Controls

- 11.1 Does the software allow the creation of user IDs with the same name, more than once?
- 11.2 Does the software encrypt the passwords, one way, and store the same in an encrypted form?
- 11.3 Does the software display the password, as it is keyed in?
- 11.4 Does the software lock the user ID, if it is used three unsuccessful times, to logon to the system?
- 11.5 Does the software force the user to change the password, at fixed, periodical intervals?
- 11.6 Does the software maintain password history, i.e. does not allow the same password to be used again, on a rotational basis?
- 11.7 Is there any audit trail for the maintenance of user profiles?
- 11.8 Does the software have provisions to create and maintain user IDs, based on the users' designations and positions held?
- 11.9 Can DBA change others' passwords? If so, is it reflected in the audit trail?

- 11.10 If a user ID record is deleted, does the software delete it physically or logically? Is the software capable of producing a report, of logically deleted user IDs?
- 11.11 Does the software have provisions to restrict different menu options, to different user IDs, based on user level (based on designation/powers, etc.)?
- 11.12 Does the software have provisions for defining access rights to users, such as, read only, read and write, modify, delete, etc.?
- 11.13 Who is in charge of user profile maintenance? Does the system provide facilities to general users to also perform such maintenance?
- 11.14 Does the software, tag each and every transaction, with the user IDs of the maker and the checker?
- 11.15 Does the software allow the same user to be both, maker and checker, of the same transaction? If so, does the software produce an exception report of transactions, with the same, maker and checker IDs?
- 11.16 Are the user IDs part of the contents, of the report printed?
- 11.17 Does the software allow automatic logical deletion of inactive users, after a certain period of time?
- 11.18 Does the system maintain that password length should be a minimum of 6 or 8 characters, or as indicated in the password policy?
- 11.19 Can user IDs be created, without passwords?
- 11.20 Does the system, limit the maintenance of system control parameters, to only a privileged user level, having sufficient authority?

Input Controls

- 11.21 Is each transaction is recorded in a way that will subsequently help establish that it has been input (e.g. Tran ID, etc.)?
- 11.22 Does the software have controls to ensure that all recorded transactions are:
 - Used as input in the system and accepted once, and only once
 - If transactions are rejected, they are reported
- 11.23 Are there adequate procedures to investigate and correct differences or exceptions that have been identified? Are there adequate procedures to investigate and if necessary, correct the following:
 - Missing and possible duplicate transactions, disclosed by the input control
 - Rejected items

566 *Information System Audit and Assurance*

- 11.24 If corrections are made to rectify differences, exceptions, duplicate transactions, missing transactions, and rejected items, are these corrections approved (e.g. maker/checker, exception report, etc.)?
- 11.25 If the input of data is through batch upload, does the software have controls, to ensure that all the entries in the batch have been uploaded, without any omission/commission (e.g. reconciliation of control totals, etc.)?
- 11.26 Does the software have adequate controls to ensure that data have been accurately input (e.g. range checks, validity checks, control totals, etc.)?
- 11.27 Verify the controls to ensure compatibility of data, when they are input in two or more modules and are correlated. For example, if the customer category, in customer master, is stated as “Staff”, then the rate of interest in the account master, for the same customer, should have an appropriate code, applicable to the staff and the system should not allow use of other codes.
- 11.28 Verify the consistency/concurrency of user inputs, if two users are accessing the same record, at the same time.
- 11.29 Verify if the inputs can be captured for various conditions (e.g. if signatures can be captured for single A/c, joint A/c, etc.).
- 11.30 Verify the controls over the system-generated transactions, through user processes (e.g. verification of outputs, containing system-generated transactions and authentication by branch officials).
- 11.31 If user controls are relied on, to ensure control over, complete and accurate input of data, are these controls adequate and operative, continuously?

Processing Controls

- 11.32 Does software have adequate controls to ensure that all transactions input, have updated the files?
- 11.33 If user controls are relied upon to ensure control over complete and accurate update of files, with data, are these controls adequate and operative, continuously?
- 11.34 Are there adequate procedures for investigation and correction of differences or exceptions, identified by the controls over, update for completeness and accuracy?
- 11.35 How such corrections been approved?

- 11.36 List out the events that cause transactions to be generated (e.g. input of a parameter such as a date, attainment of a condition, etc.), the key data used, as a basis for such generation and the programmed procedures that perform the generation. (e.g. in an interest calculation process, generally, the user runs the interest run job, the system takes the customer balances (key data), applies interest rates (key data) and debits/credits the interest. The program, which performs these activities, should be logically sound, so that no processing errors are caused).
- 11.37 For the key data outlined above, are there adequate controls, to ensure that the key data that is used as a basis for the generation of data, is complete and accurate?
- 11.38 Where applicable, is the key data authorised by the appropriate level of users and kept secure?
- 11.39 For the programmed procedure that generates the data, if user controls are used, to check the accuracy of the generation process, will these be adequate?
- 11.40 Are there adequate procedures to investigate and correct any differences or exceptions, identified by the controls, over the completeness and accuracy of generation? Have the corrections been approved?
- 11.41 Is there any restart facility for batch jobs, if they are terminated abruptly? Are there controls to ensure that no errors occur during restart?
- 11.42 Is the user ID of the person who executes the batch job, embedded in the transactions?
- 11.43 If the process has to be done only once, does the software ensure that the process is not executed, more than once?
- 11.44 Is there any day-begin, day-end process? If so, are these processes logically sound to carry out the designed objectives, completely and accurately?
- 11.45 Are the transactions for the day, identifiable?
- 11.46 Does the software ensure sequencing of processes, i.e. does the software ensure that processes are not initiated out of sequence?
- 11.47 If certain processes are compulsory, does the software ensure that all such processes are completed, before triggering the day-end process?
- 11.48 Verify if there is an event log for the batch processes.
- 11.49 Verify if the application is able to handle processing at peak times (e.g. is the application capable of handling tasks that progressively increase in volume).

568 *Information System Audit and Assurance*

- 11.50 Verify if the software maintains audit trail, to uniquely trace any modification/ deletion/addition, with the user ID.
- 11.51 If updates occur in more than one file or table, and if the process is interrupted, verify if there is a provision for roll back.
- 11.52 Verify if the application maintains adequate control over security items such as, DDs/pay orders/branch advices, etc.? Are they reconciled and exceptions if any, identified and reported?

Output Controls

- 11.53 Verify the format, contents, accuracy, and utility of the reports, generated by the system.
- 11.54 Verify if there is any provision for generating exception transactions statement, from the system.
- 11.55 If the output has a high number of pages and if printing is interrupted, is there any provision to restart printing from that page?
- 11.56 Verify if output can be viewed/generated by users, only on a 'need to know' basis. In other words, check whether outputs cannot be generated, by all and sundry users, in the system.
- 11.57 Check the controls exercised by the user (branch/office) on the generation, distribution, authentication, and preservation of computer output and comment on the adequacy of the same.
- 11.58 Check whether the application is keeping adequate controls over computer-generated output lying in the print queue/spool.
- 11.59 Does the output contain key control information, necessary to validate the accuracy and completeness of the information, contained in the report such as, last document reference, period, etc.?

Interface Controls

- 11.60 If the data has to be transferred from one process to another verify if manual intervention is possible or if unauthorised modification to data can be made.
- 11.61 Verify the mode of transfer of data, from one process to another, i.e. through floppy or mail.
- 11.62 Verify the effects caused, when one process is down and the interface is working.
- 11.63 Is there a periodic system, of ensuring consistency of data, from the process from which it is transferred to the process it is transferred to?

Authorization Controls

- 11.64 If the transaction is authorized by the software itself, under specific conditions, are the programmed procedures logically sound, to ensure that all authorizations take place only as expected?
- 11.65 Does the software, prevent the same user, from performing both, the functions of entering a transaction and verifying it?
- 11.66 If transactions are authorized manually, are there controls to ensure that:
 - (a) they are properly authorized, by an independent and responsible official, and
 - (b) no unauthorized alterations are made, to the authorized transactions?
- 11.67 In cases where manually approved transactions are authenticated by the input of a password, are the passwords adequately controlled?
- 11.68 Do access rights, reflect the appropriate authority limits?
- 11.69 A transaction is identified by the system, as requiring supervisory approval and is consequently, routed to a queue file pending review and then, released by a responsible official. In this case, are the procedures for identifying 'items needing approval', adequately equipped, to identify such transactions?

Data Integrity/File Continuity Controls

- 11.70 Is hash total used, to verify the continued integrity of data? Is the total, of the items on data file, regularly reconciled to an independently-established total, e.g. agreement to a manual control account, or computer agreement to a control record, on a suitable, timely basis, to ensure that there is no tampering of data?
- 11.71 Are adequate procedures in place, to investigate and correct the differences, disclosed by the above-mentioned reconciliation exercise?
- 11.72 Verify if the entire record, after commit, can be physically deleted (it should not be allowed though).
- 11.73 If the software keeps a record of security items, are there adequate controls, to ensure the complete and accurate recording of security items in the system?
- 11.74 Are the programmed procedures, which utilize the security items in the system, logically sound, so that there are no errors?
- 11.75 Are all asset movements, supported by suitable, written authorizations?

12. DATABASE CONTROLS

It is important to ensure the following, with reference to databases:

- Database is physically secure and free of any corruption
- Access to the database is restricted, and permitted only to authorized personnel
- Referential integrity of the data is ensured at all times
- Accuracy of the contents of the database, is verified periodically
- Database is technically verified, periodically, in terms of, storage space, performance tuning, and backup
- Backups of the database are periodically retrieved and it is ensured that they are in order

The database control checklist, is divided into the following areas:

- Physical access and protection
- Referential integrity and accuracy
- Administration and house-keeping

Physical Access and Protection

- 12.1 Is there a list of databases, with the names of administrators who are recognized by the bank?
 - (a) Mission critical systems such as Internet banking, core Banking, etc. ATM base 24 database
 - (b) Essential systems such as, credit card processing systems (which operate on the near online mode)
 - (c) Reporting systems such as data warehouse, EIS reporting
- 12.2 Is responsibility shared by the user department and the IT department for the administration of mission critical databases?
- 12.3 Does the IT department identify and segregate the hardware, hosting these databases and have these hardware resources been earmarked?
- 12.4 In cases where the same hardware, is used at branches or other locations, is there a clear partition between application area and data area?
- 12.5 Does the IT department have laid-down standards/conventions for database creation, storage, naming, and archival?
- 12.6 Are database administrators, placed at responsible levels, in the bank?

- 12.7 For database access, are the OS level file and directory permissions restricted, as required for the application?
- 12.8 Are users denied access to the database, by ways other than, through the application?
- 12.9 Is the use of triggers and large queries monitored, to prevent overloading of database and consequent system failure?
- 12.10 Are direct query/access to database, restricted to the concerned database administrators?
- 12.11 Are all vendor-supplied passwords, given to the default users, changed? Have all demo users and demo databases been removed?
- 12.12 Are there controls to check sessions per user, number of concurrent users, etc.?
- 12.13 Is the creation of users, restricted and need-based? Are the rights, granted to various users, reasonable and based on requirement?
- 12.14 Is the database, configured to ensure audit trails, logging of user sessions, and session auditing?
- 12.15 Does the administrator maintain a list, of batch jobs executed on each database, severity of access of each batch job, and timing of execution?
- 12.16 Are batch error logs reviewed, and corrective action taken, by the administrator, periodically?
- 12.17 Is there a separate area, earmarked for temporary queries, created by power users or database administrators, based on a specific user request?
- 12.18 Are, temporary sub-databases created, removed periodically, or after the desired purpose is achieved?
- 12.19 Does the design or schema of all tables/ files in the database, contain fields for recording makers, checkers, and time stamp?
- 12.20 Are database administrators rotated periodically?
- 12.21 In cases where customer data is provided to external service providers, does the bank have undertakings from these service providers to maintain confidentiality?

Referential Integrity and Accuracy

- 12.22 Are there a standard set of database control reports, designed in consultation with the user department, for ensuring accuracy and integrity of the databases?

572 *Information System Audit and Assurance*

Examples:

- (a) Total of transactions and balances
 - (b) Record counts
 - (c) Hash totals
- 12.23 Are these reports, run periodically, directly from the backend database and are the results, both, positive and negative, communicated by the administrators to the senior management personnel?
- 12.24 Are these reports run periodically, and taken directly, by the user department itself, to ensure accuracy?
- 12.25 In case of automated interface between systems, is there a system of reconciliation between the source and the receiving system, for critical information?
- 12.26 Is there a system of periodic reconciliation, between the sub-databases and the GL database of the bank?
- 12.27 In cases where data is migrated from one system to another, has the user department verified and is it satisfied, about the accuracy of the information, migrated?
- 12.28 Is there, a formal data migration report?
- 12.29 Are there entries, directly made to the backend databases? If they are made under exceptional circumstances, is a system of written authorization in place?
- 12.30 If entries in the database are updated/ deleted due to any exceptional circumstances, e.g. during troubleshooting, etc., are these changes approved, in writing and then recorded?

Administration and House-Keeping

- 12.31 Does the system administrator, periodically review, the list of users of the database? Is the review documented?
- 12.32 Are inactive users deactivated?
- 12.33 Is there a backup schedule?
- 12.34 Are databases periodically retrieved from the backup, in a test environment and is accuracy ensured, in the physical environment?
- 12.35 Are senior personnel from the user department, involved in testing backup retrieval?
- 12.36 Is there periodic purging/archival of databases?

13. NETWORK MANAGEMENT

Process

- 13.1 Is there an information security guidelines document, which defines the minimum configuration for any device/link, on the bank's network, including levels of encryption?
- 13.2 Are all platforms/links/devices, in compliance with the guidelines? If not, has an appropriate level of management, reviewed the non-compliant parts of the network, to ensure that the risks levels are brought down to acceptable levels?
- 13.3 For all items supported by external vendors, does the vendor or the manufacturer verify if all cryptographic functions, in use by the product/service, such as, encryption, message authentication, or digital signatures, use the cryptographic algorithms and key lengths approved by the corporate IT department?
- 13.4 Wherever applicable, are the background and reference checks, for both, internal and outsourced vendor staff, who perform security-related functions, for the product/service under review, carried out? This includes, job applicants who have accepted a job offer, temporaries, consultants, full-time staff, as well as the outsourced vendor, who is involved in product/service management and operations.

Risk Acceptance (Deviation)

- 13.5 Does the bank have a risk acceptance process, wherein, all the identified risks are documented, and approved for any non-compliant issue, that cannot be remedied and where effective compensatory controls exist?

Authentication

- 13.6 Does the product/service, authenticate (verify) the identity of users (or remote systems), prior to initiating a session or transaction? Have these authentication mechanisms, been approved by the bank's IT department? (these include Personal Identification Numbers (PINs), passwords (static and dynamic), public keys and biometrics.)
- 13.7 Does the bank, verify if the initial authentication has used a mechanism that is acceptable for the application? Has the approach been approved by IT department and have the required compensating controls been implemented?

Passwords

- 13.8 Does the bank have a comprehensive, password construction, implementation, and management policy?

Personal Identification Numbers (PINs)

- 13.9 Does the bank have a policy for Personal Identification Numbers, used by various sets of customers, who access the bank's systems directly, using channels like ATM, phone banking, Internet banking, mobile banking, etc.?

Dynamic Passwords

- 13.10 Do the products/services, using dynamic passwords for authentication, use an IT department-approved authentication server, to validate the password?

Public Key Infrastructure (PKI)

- 13.11 Do the products/services, using public key (or asymmetric) cryptography for authentication, either on a session basis (peer authentication), or on a per-message/transaction basis (digital signatures), use approved security protocols, to comply with the public key technology standard?
- 13.12 For products/services that use PKI, private keys which are stored in hardware or software, must be protected via, an approved mechanism. The protection mechanism includes user authentication, to enable access to the private key.
- 13.13 For products/services that use PKI, an approved process, for verifying the binding of a user identity to the public key, e.g., digital certificate, is required for any server, relying on public key authentication.

Biometrics Authentication

- 13.14 Do the products/services, utilizing biometrics authentication, use only biometrics for local authentication?

Access Control

- 13.15 Is the access to highly privileged IDs, e.g. system administration access, strictly controlled, audited, and limited in its use?
- 13.16 Does the product/service, support the need to perform a periodic entitlement review? A periodic entitlement review process, should validate access privileges.
- 13.17 Does the product/service, support the requirement to limit, individual user sessions to a maximum of X minutes of inactivity, using either, session time out or a password-protected screen saver.
- 13.18 Is there a process in place, to ensure that access rights reflect the changes in employee or job status, within X hours of the change? This includes physical access tokens and dial-in capabilities, as well as any system or application.
- 13.19 Does the product/service, support the ability to disable external customer, user IDs, after X months of inactivity and delete these after Y months of inactivity, unless they are extended, through the explicit, written approval of the business.
- 13.20 For any product/service, which has been outsourced, is there a process in place, to ensure that all platforms, services and applications are configured, to meet the bank's information security standards?
- 13.21 Does the product/service display:
 - (a) the date and time of the last successful login, and
 - (b) the number of unsuccessful login attempts, since the last successful login.
- 13.22 Does the product/service, support a periodic process, to ensure that all user IDs for employees, consultants, agents, or vendors, are disabled after X days and deleted after Y days, from the day they were stopped being used, unless, explicitly approved by the business.

Cryptography

- 13.23 Is there a cryptography/encryption policy, for various types of classified information that travels/gets stored, within and outside the bank's network(s)?

NETWORK INFORMATION SECURITY

- 13.24 Have the Network data-monitoring tools, e.g., sniffers, datascopes, and probes, utilized by the product/service, been approved by the bank's IT department?
- 13.25 Is the approved legal affairs banner, being displayed at all entry points, where an internal user, logs into the product/service? An automated pause or slow roll rate, is put in place, to ensure that the banner is read. The legal affairs banner, usually, carries the following kind of text:
- “You are authorized to use this system for approved business purposes only. Use for any other purpose is prohibited. All transactional records, reports, E-Mail, software, and other data, generated or residing upon this system, are the property of the company and may be used by the company for any purpose. Authorized and unauthorized activities may be monitored.”
- Note:* This is required for all mainframe, mid-range, workstation, personal computer, and network systems.
- 13.26 Has dial-in connectivity been prohibited on a network-connected machine (server and workstation), except, where documented and explicitly approved, in writing, by the business management and the IT department? When explicitly approved, the modem must, as a minimum control, prohibit answer or pickup, until after the 5th ring.
- 13.27 Have the remote control products, used in a dial-in environment, been approved by the IT department, explicitly?
- 13.28 Has it been ensured that only the software (applications/operating systems, etc.), supported by only the vendors, are used? (unsupported software could be vulnerable to attacks, since the vendors would not come up with the relevant patches.)
- 13.29 Is the antivirus software, configured to check viruses, even from the floppy drive/CD ROM drive?

E-Mail and Voice Mail: Rules and Requirements

- 13.30 Is there a policy that covers E-Mail and voice mail transmission of data?
- 13.31 Are there procedures, which require that all the incoming E-Mail messages be scanned for viruses, to prevent virus infection in the bank's network?

- 13.32 Are all E-Mails, identified with a user's name or E-Mail ID, to facilitate tracking? Is the E-Mail ID, allotted to a user, prevented from being used by another user?
- 13.33 Ensure that users do not forward the E-Mail messages automatically, without prior approval.
- 13.34 Are there procedures to ensure that users do not send confidential or sensitive information via, E-Mail? Is the information, transmitted through E-Mail, encrypted?
- 13.35 Are all E-Mails, sent and received by employees via the bank's network, treated as the bank's records? Is there a procedure to monitor them?

Information Security Administration

- 13.36 Is there an approved document, clearly outlining the Information Security Administrator's (ISA) responsibility?
- 13.37 Are all the administrative actions e.g., adding/ deleting users, changes to entitlements/ passwords, backedup by an independent review?
- 13.38 Does the ISA function, review all security audit logs, incident reports, and online reports, at least once, per business day?
- 13.39 In case of Wide Area Networks (WAN), are the router tables maintained securely, in routers?
- 13.40 Are router login IDs and passwords, treated as sensitive information and managed by authorized administrators?
- 13.41 Are all changes to router table entries, logged and reviewed independently? Are access violations taken note of, forwarded to a higher authority and acted upon, in a timely manner?
- 13.42 Is there a process, to report all unusual or suspicious activity? (Reporting to the IT department, investigating immediately and bringing the case to closure, without delay)?
- 13.43 Does the ISA function, assess compliance with their security procedures, quarterly and does it report their results to the IT department?
- 13.44 Have all the security-related administrative procedures, under the control of the ISA, been documented and approved by the management (annual exercise)? At the minimum, procedures should include:
 - Information ownership
 - Data classification
 - User registration/ maintenance

578 *Information System Audit and Assurance*

- Audit trail review
- Violation logging and reporting
- Sensitive activity reporting
- Semi-annual entitlement reviews
- Password resets
- Escalation reporting

Microcomputer/PC Security

- 13.45 Do the LAN servers, mail servers, and microcomputers, have IT department-approved antivirus products, installed?
- 13.46 Are all product/service-specific microcomputers/PCs, secured against removal and theft, commensurate with the value of the computer and the information it holds, along with a process that helps report any theft, to the IT department?
- 13.47 Are microcomputers/PCs, having sensitive information, protected with power on password, to prevent unauthorized access?
- 13.48 Are, sensitive data in such microcomputers/PCs, backedup and preserved properly, with records, to ensure recovery, in case of failure?

Audit Trails

- 13.49 Does the audit trail, associated with the product/service, support the ability to log and review all actions, performed by the system operators, system managers, system engineers, system administrators, highly privileged accounts, and emergency IDs?
- 13.50 Do the financial transactions, as well as additions, changes, and deletions to a customer's demographic data/important statistics, get recorded in the product/service audit trail?
- 13.51 Does the audit trail for product/service, record all identification and authentication processes? Also, is there a retention period for the audit trails?
- 13.52 Does the audit trail, associated with the product/service, log all actions performed by the ISA?
- 13.53 Is there a process in place, to log and review all the actions performed, by system operators, system managers, system engineers, system administrators, security administrators, and highly privileged IDs?
- 13.54 Is there a process in place, to log and review the actions performed, by emergency IDs, associated with the product/service?

Violation Logging Management

- 13.55 Is the product/service, capable of logging the minimum criteria, specified to log and report, specific security incidents and all other attempted violations of system integrity?
- 13.56 Are the product/service owners aware of their responsibilities, with respect to security incident reporting?

Information Storage and Retrieval

- 13.57 Have all the media (File/Floppy/Disks, etc.), under the control of the product/service owner, been classified and securely stored, with access restricted to authorized personnel only?
- 13.58 Is there a process in place, to ensure that all media, under the control of the product/service owner, containing critical information, is destroyed in a manner, that renders it unusable and unrecoverable?
- 13.59 Is there a procedure in place, that enforces and maintains, a clean desk program, which secures all critical information from unauthorized access?

Penetration Testing

- 13.60 Has it been ensured that the products/services, which use the Internet for connectivity or communications, have undergone a successful penetration test, prior to production implementation?
- 13.61 Is there a penetration test process that ensures that the modifications to the product/service, which uses the Internet, for connectivity or communication, have been reviewed, to determine whether or not a subsequent penetration test is warranted?
- 13.62 Is there an Intrusion Detection System in place, for all the external IP connections?

14. MAINTENANCE

Maintenance will include the following:

1. Change request management and version control
 - Software developed in-house
 - Software purchased from an outside vendor

2. Software troubleshooting
3. Backup and recovery
4. Hardware maintenance
5. Training

Wherever the application service provider, who owns the hardware and maintains the OS/application software, processes the data for the user, a detailed Service Level Agreement should be prepared, covering the entire maintenance.

Change Request Management and Version Control

Software Developed In-house

- 14.1 Check if requests for changes, are initiated by users, in a structured Change Request Form (CRF), with pre-printed numbers.
- 14.2 Are these change requests, inwarded in a manual/electronic register with the CRF number, before initiating the change.
- 14.3 Are the change requests, subjected to a feasibility study?
- 14.4 Verify that the change request is approved by the management, before effecting the changes in the software, and that the same is recorded, on the CRF.
- 14.5 Verify that the changes are made, only in the test environment and not in the live environment (separation of test and production libraries).
- 14.6 After making changes, are they tested adequately, before implementation (unit testing, integrated testing, regression testing, etc.)? All these testing procedures should happen, only in the test library.
- 14.7 Once the programs are ready after testing, are they approved by a senior programmer/ departmental head? Are such approvals, recorded on the CRF?
- 14.8 After approving the changes, are the changed programs transferred to the production library, by an independent person, who does not have programming/ development responsibilities?
- 14.9 Does the production library have both, sources and executables, of the latest version of the programs?
- 14.10 Check whether the programmers are given access to the production library. Similarly, check whether the access to the test library, is restricted to programmers alone.

- 14.11 Verify if the changes have been updated in the user, technical, operations, and all other relevant manuals, to reflect the current state of the software. Has the CRF been updated, to this effect?
- 14.12 Verify if implementation guidelines are prepared by the programmers, for properly implementing changes in the user sites. Have they been approved?
- 14.13 Verify if the changes are implemented at the users' sites, in accordance with the implementation guidelines. Has the CRF been updated, to this effect?
- 14.14 After completing all these steps, is the open entry, in the change request register, rounded off for the relevant CRF number, to bring it to a logical conclusion?
- 14.15 Is the completed CRF, filed along with the system documents?
- 14.16 Are there procedures, to review and monitor all the pending change requests and initiate timely action, to resolve the same?

Version Control

- 14.17 Verify the procedure for roll out of software to the users' sites. Check who is creating the executables from the changed source code, for implementation in the user sites? Ensure that that such person(s) is/are independent of development activities.
- 14.18 Verify that the access to the compilers, is restricted to only authorized persons, who are empowered to create the executables from the source code.
- 14.19 Check whether identity of different programs is maintained between any two software releases and each release contains all the changes to different programs, from the previous release.
- 14.20 Check whether each release is given a version number.
- 14.21 Verify if proper records are maintained, to reflect the different version numbers of the software, their composition, and location. The latest version should be capable of being easily differentiated, when compared with the older versions.
- 14.22 If possible, take the latest version of any one program in the test library and arrange to compile the same, to arrive at the new exe file. Note down the byte size of the new 'exe' file and compare whether the byte size of the exe program in the live area, in the user site, is the same as the size that has been noted.

582 *Information System Audit and Assurance*

- 14.23 If multiple user sites exist, verify the control mechanism, to ensure that the same software is being implemented, in all such user sites.
- 14.24 If there are exceptions to certain users, verify if such exception modules of the software, are kept in the central control library, from where, the software is rolled out.
- 14.25 Verify if there is any register/ database, containing information on which site has which version.
- 14.26 Check and ensure that backup of all versions of the software, are held both, onsite and off-site, in fire resistant cabinets, with proper records.

Software Procured from Outside Vendor

- 14.27 Verify if there is an annual maintenance contract for the software and check whether it is currently, in force.
- 14.28 Check if requests for changes are initiated by users in a structured Change Request Form (CRF), with pre-printed numbers.
- 14.29 Verify if the change request is approved by the management, before asking the vendor to effect the changes in the software.
- 14.30 Are these Change Request Forms (CRFs) inwarded in a manual/ electronic register, before sending it to the vendor, for making changes.
- 14.31 For all the changes, effected and implemented by the vendor, check whether release notes have been provided for all such patches/ releases. If so, do the release notes, given by the vendor, contain the CRF number, submitted by the bank.
- 14.32 Check whether the release notes have been circulated among all the users.
- 14.33 Check whether the open entry in the inward register, having the CRF number, attended by the vendor, has been rounded off, to reflect the latest pending position.
- 14.34 Check whether the vendor has updated the user and operations manuals, to reflect the current state of the software, and also, if the vendor has delivered the same, to the bank.
- 14.35 Check the procedure for marking off entries, in the inward register for CRFs, maintained at CPPD/IT and ensure that the current list of outstanding requests, are complete and accurate.
- 14.36 Is there a procedure to review and monitor all the pending change requests and initiate timely action, to get the same, resolved by the vendor, in a time-bound manner.

- 14.37 Verify the Service Level Agreement (SLA), with the vendor. Does it lay down the basis of billing, i.e., is it based on 'x' number of lines of coding, or on 'y' number of man hours of effort?, etc. Check whether the billing, made by the vendor, is in accordance with the SLA. Test check to see whether the billing raised, is accurate.
- 14.38 Does the SLA have a penalty clause, for delay on the part of the vendor in delivering the changes, after submitting the CRF? If so, for any delays, on the part of the vendor, does the bank invoke the penalty clause and charge a penalty?
- 14.39 Verify, if any escrow arrangement exists, for the source code. If so, check who the escrow party is inspect their site and check if a copy of the latest version of the source code is stored there, in proper condition, with records.
- 14.40 Check if a copy of the full set of the latest documentation of the software, is also kept with the source code, in the escrow's location.
- 14.41 Check and ensure that the escrow party does not have unilateral access, to the source code and documentation, without the knowledge of the software vendor and the bank.
- 14.42 Check and ensure that backup of the latest version of the software, provided by the vendor, is held both, onsite and offsite, in fire resistant cabinets, with proper records.

Software Troubleshooting

Help Desk

- 14.43 Check if user calls are logged in a register (manual or electronic), in the help desk, with a unique identification number for each call. Preferably, the numbering should be serially done and must be unique for each user site.
- 14.44 Is this number recorded in a help desk register, in the user's site along with details of the nature of the call, date, and time of call?
- 14.45 Does the help desk register in the user site, reflect all the call identification numbers serially, without any missing number, in between?
- 14.46 Are the date and time of resolving the trouble, recorded in the help desk register? Do they correspond to and tally with, the records maintained at the help desk?
- 14.47 Are the calls attended to, in a timely manner?

584 *Information System Audit and Assurance*

- 14.48 Do the help desk issue a call sheet, with solutions given, duly signed by the user?
- 14.49 If troubleshooting is attempted by the help desk personnel check whether any sensitive password was divulged by the user, to the help desk. This should have been recorded in the help desk register both, at the user site and at the help desk.
- 14.50 If a sensitive password is revealed to the help desk, check the system and application logs, and ensure that the changes made, are appropriate, to deal with the trouble reported by the user.
- 14.51 Check if the command log, is printed and submitted to the user site, duly signed by the help desk official and authenticated by the help desk in-charge.

File/Data Reorganization

- 14.52 If the software works on a RDBMS, check whether file/ database reorganization is carried out at the user site, on time, to avoid any processing error.
- 14.53 If any addition to datafile/ tablespace is made, is it approved and in accordance with the software implementation guidelines?
- 14.54 If operating system/ database fine tuning is carried out, are these documented in the error log/help desk register?
- 14.55 As most of these activities require sensitive passwords, is the usage of the same, recorded in the password usage register, duly signed by the support personnel and user?
- 14.56 Verify the command logs and ensure that the command and command results, are appropriate for file/ database reorganization/ fine tuning, etc.
- 14.57 Verify if due to O/S upgrades, any constraint is noticed in the application software.
- 14.58 Verify if the interface software, is properly tested and implemented, if the user is using 2 or 3 applications and the data is transmitted through this interface application.

Backup and Recovery

Software

- 14.59 Verify if the latest copy of the backup of software (operating system, RDBMS, application, etc.) has been made, and preserved at the user site.

Data

- 14.60 Verify if different types of data backup are taken periodically, at specified intervals, as advised by the software developer/vendor.
- 14.61 Are there proper records for making not of the media in which, different data backups are stored, data type, the location, where it is stored, date of backup, due date for recycle, etc.
- 14.62 Has a copy of the data backup been kept in an offsite location, with proper records?
- 14.63 Does the database/system administrator, at the user site, carry out restoration testing of these backups, periodically? Also is it recorded and authenticated?
- 14.64 Are users involved in such restoration testing?

Purging of Data

- 14.65 Verify if there is an archival policy, and if data house-keeping is done, as per this policy.
- 14.66 Verify if this archival data can be read, as and when required.
- 14.67 Verify if this archival data is stored in a safe place.
- 14.68 Verify if archived data has been deleted from the current running system.
- 14.69 Verify if the printed reports have been deleted from the system.

Hardware Maintenance

- 14.70 Verify if there is any Service Level Agreement, between the hardware vendor and CPPD/IT department.
- 14.71 Check and ensure, that the AMC with the vendor, for maintenance of hardware equipments, is active and currently, in force.
- 14.72 Verify if the network diagram is available at the user site.
- 14.73 Does the user site have the names and photographs of the service personnel and are they identified by the users, before allowing them to handle the hardware?
- 14.74 Verify if the hardware inventory is maintained at the user site. Ensure that the physical stock of hardware items, matches with the hardware inventory.
- 14.75 Verify if the hardware maintenance register is maintained, with full details about, nature of trouble, date and time of reporting, name of

the vendor, engineer's name, date and time of resolution, signature of DBA, signature of engineer, initials of head of the user site.

- 14.76 Verify if there is a databank, of malfunctions of hardware. If so, examine whether similar types of hardware errors, are recurring. Check the steps taken by the users/ CPPD/ I T department to arrest this trend.
- 14.77 Before the hardware is taken by the vendors for servicing/ repair, does the user site ensure that the equipment does not contain sensitive live data?

Training

- 14.78 Verify if the users are given adequate training, on the application system functionalities.
- 14.79 Verify if the technical personel are given adequate training, of the technical details of the application system, to provide necessary troubleshooting/help, to users.
- 14.80 Verify if the users are aware of the steps to be taken, in case of a contingency, due to non-availability of systems.

15. INTERNET BANKING

Information Systems Security Framework

- 15.1 Is there a security policy, duly approved by the board of directors? Is there a segregation of duties of the security officer/group, dealing exclusively with Information Systems security and those of the Information Technology division, which actually puts into operation, the computer systems? Is the role of an information security officer, independent in nature?
- 15.2 Is the role of an Information System auditor, independent in nature? (It should be independent of the operations and technology unit).
- 15.3 A bank should ensure that the Information Systems auditor, forms part of its internal audit team.
- 15.4 Banks should acquire tools for monitoring, systems and networks, against intrusions and attacks. These tools should be used regularly, to avoid security breaches. Banks should review their security infrastructure and security policies regularly, and attempt to optimize their utility, in the light of their own experiences and changing technologies. They should educate their security personnel and also the end-users, on a continuous basis.

- 15.5 Banks should subscribe to the systems alerts/patches. The Information Systems auditor should ensure that, all vulnerable patches are applied on a periodic basis, to prevent outsiders from exploiting the Banks' systems.
- 15.6 Under the present legal requirements, there is an obligation on the part of banks, to maintain secrecy and confidentiality of the customers' accounts. In the Internet banking scenario, the probability of banks, not meeting the above obligation, is high, on account of several factors. Despite all reasonable precautions, banks may be exposed to enhanced risk of liability to customers, on account of breach of secrecy, denial of service, etc., because of hacking or other technological failures. Should the bank, therefore, institute adequate risk control measures, to manage such risks?
- 15.7 In order to address the issue of risk of liability to customers, on account of breach of secrecy, denial of service, etc. should the bank follow a privacy policy?
- 15.8 Some of the areas, which all banks need to include, as part of the privacy policy are given below:
 - Banks should safeguard, according to strict standards of security and confidentiality, any information that their customers share with them
 - Banks will not reveal customer information to any external organization, unless they have previously, informed the customer through disclosures or agreements or have been authorized by the customer, or are required to do so, by law or the regulators.
 - Whenever banks hire other organizations to provide support services, they should ensure that these organizations, conform to the privacy standards of the banks and also, allow banks to audit them, for compliance

Web Server

- 15.9 Is the web server, configured to be a stand-alone unit, without any membership, to any domain inside the bank's IT architecture?
- 15.10 Ensure that the web server is ported with the latest versions of patches and service packs. Usually, the OS vendor releases patches and service packs, with appropriate fixes, to prevent Denial of Service (DOS) attacks. These should be applied, to prevent such attacks on the web server.

588 *Information System Audit and Assurance*

- 15.11 All security settings, applicable to the operating system, in which the web server operates, should have been implemented, as per the IT security policy. Check and ensure this.
- 15.12 With regard to the super user account:
 - Check whether the super user account in the web server, is enabled for login, only on the system console and not from across the network. This is applicable to all user accounts in the web server
 - Check if appropriate parameters are implemented, in the operating system of the web server, so that the super user account will lock out, if too many unsuccessful attempts are made across the network, but will remain unlocked, at the system console
- 15.13 Ensure that sensitive operating system-related, executable program files and data files on the web server, are not stored in public area, but in any other secure location, with audit, duly enabled.
- 15.14 IP routing should be disabled in the web server. Check and confirm this.
- 15.15 Ensure that unauthorized ports, for, e.g. UDP port No.443, are not allowed inside the web server. Also, ensure that unnecessary services like, ftp, messenger, SMTP, telnet, etc. are not installed and are inactive on the web server.
- 15.16 The facility to shutdown the machine should be restricted to the system console, on the web server. Check and ensure this.
- 15.17 Access to floppy drive, CD-ROM drive, etc. should be restricted in the web server, to interactive only, to prevent these devices from being shared by all the processes on the system. Check and ensure this.

Logs of Activity

- 15.18 Ensure that auditing is enabled in the web server's operating system and check if the logs are reviewed and authenticated, by authorized officials, periodically.
- 15.19 Check if audit trail is enabled on the firewall, to log the changes made, to the rule base settings and verify if the logged entries are approved by higher authorities in the IT department.
- 15.20 Are the system administrators, monitoring the logs, produced by the Intrusion Detection System (IDS) (an Intrusion Detection System, helps in recognizing security threats and is capable of scanning packets, to check for vulnerabilities. It ensures that Distributed Denial of

Service attacks, are prevented) and also bringing the access violations, to the attention of the senior-level management in the IT department, for guidance. Are these documented and is appropriate corrective action taken?

- 15.21 Check whether audit trails are enabled for administration activities, and whether entries logged in the audit trail, are in accordance with the process flow chart and if no unauthorized activity has been carried out.

Demilitarized Zone and Firewall

- 15.22 Are all Internet connections routed through a firewall? Does a dedicated team, manage the firewall? Are the ports opened, only on a “need to have” basis?
- 15.23 Has an Intrusion Detection System (IDS) been implemented?
- 15.24 Are the application and database servers kept separated, from the web server, in the demilitarized zone?
- 15.25 Is the demilitarized zone separated from the Internet cloud, by means of a firewall? (Firewall procurement should be through an approval mechanism, which ensures that only firewalls of the highest standards, are procured).
- 15.26 If the demilitarized zone is connected to the Intranet within the bank, it should be separated by a firewall. Check and ensure the same.
- 15.27 Check whether the firewall rule base is treated as sensitive information, and knowledge of the same is restricted to authorized officials in the IT/computer operations department alone.
- 15.28 Ensure that the decision to open specific firewall ports/rule base is approved, in accordance with the IT security policy (IT security policy should list out such ports), e.g. firewalls should block unwanted ports that are running services such as, ftp, telnet, SMTP, etc. in the demilitarized zone. Ideally, only http and https ports should be allowed. Check and verify this.

Security Review of All Servers Used for Internet Banking

- 15.29 Carry out an operating system security review, on all the servers used for Internet banking, apart from web server, and ensure that all security parameters have been properly set as per the security policy.

Database and System Administration

- 15.30 Has the bank appointed a database administrator, with clearly defined roles?
- 15.31 Has the bank appointed system administrator(s), with clearly defined roles?
- 15.32 Check whether process flow of administration activities is documented and approved by the head of operations and also if the administrators are conversant with the process flow.
- 15.33 Carry out an application control review of the administration module and ensure that the functionality, as described in the process flow document, is adequately met with by the module.
- 15.34 Examine who has access to the super user account in the administration module. Examine the procedures for custody and usage of password and records maintained, for the same. Are all usages recorded by the administrator and authenticated by appropriate authority?
- 15.35 Obtain a list of all administrator accounts in the administrator's module and check whether all are attributable to personnel engaged in administration. Extraneous administrative IDs should be identified and reported for deletion.
- 15.36 Check whether the menu options in the administrative module are assigned to different administrators, on a need to know basis, based on functionality offered by the menu options and the work allotment made to the administrator.
- 15.37 Obtain the list of menu options in the Internet banking module for customers and check whether such menu options are assigned to user (customer) IDs, only as per their request and as per the policy of the bank.
- 15.38 Pay particular attention to user (customer) IDs, which are provided for, by third-party funds transfer facility on the Internet and verify whether they are backed by proper customer request, in writing.
- 15.39 Does the bank have a proper infrastructure and schedules for backing up data? Is the backed up data periodically tested, to ensure recovery without loss of transactions in a time frame, as given in the bank's security policy? Is business continuity ensured by setting up disaster recovery sites? Are these facilities tested periodically?
- 15.40 Check the procedure for creation of different user accounts for the customers, for usage on the Internet and whether they are backed by valid customer requests, for such a facility.

Operational Activities

- 15.41 Considering the prevalent legal position, has it been ensured that the banks not only establish the identity, but also make enquiries about the integrity and reputation of the prospective customer? Also, is it ensured that even though request for opening an account can be accepted over the Internet, accounts are opened only after proper introduction and physical verification of the identity of the customer? Is there a legal contract with the customer in place, covering the risks of communication, using the public network?
- 15.42 Pay particular attention to customers whose constitution is other than “individual”, particularly corporate accounts and check whether appropriate account-opening documentation has been submitted by such customers for Internet banking.
- 15.43 Check if any customer has been provided multiple user IDs, especially if he/she is not a joint account holder.
- 15.44 Any account linkage activity should take place only after ensuring that the user accounts are created, based on valid customer requests.
- 15.45 Check if user IDs are linked to multiple bank accounts. If so, verify whether such accounts pertain to the same customer.
- 15.46 Check the procedure for enabling the customer user ID on the Internet and verify whether adequate precautions are taken by the operations personnel, to identify the customer before enabling the ID. The account enablement process should be decided and signed off, before product launch. The entire process should be auditable and audit trails should be enabled for the same (each bank can decide whether it can pre-enable or post-enable the user accounts, based on its individual policy).
- 15.47 Check the procedure for creation of new password for customers, who report having forgotten the password. Verify the procedure for ensuring the identity of the customer, before creating the new password.
- 15.48 Verify whether adequate records (either electronic or manual) are maintained for the customer user IDs that have been created, enabled, new passwords provided for, etc. and whether they are authentic. Test check the instances of change of customer’s passwords and whether they are backed by valid customer requests.
- 15.49 Do all applications of banks have proper record-keeping facilities, for legal purposes? It may be necessary to keep all received and sent messages, both encrypted.

Application Control Review of Internet Banking Application

- 15.50 Does the software allow creation of user-IDs in the same name, more than once?
- 15.51 Does the software encrypt the passwords one way and store the same, in encrypted form, in the database?
- 15.52 Does the software display the password, as it is keyed in? (It should not be displayed on the screen).
- 15.53 Does the software lock the user ID if it is used for X unsuccessful times, to logon to the system?
- 15.54 Does the software force the user to change the password at set, periodic intervals?
- 15.55 Does the software maintain password history, i.e. the same password should not be used again, on a rotational basis.
- 15.56 Check whether the software, logs the instances of change of user's (customer's) password in the audit trail.
- 15.57 Does the software allow automatic logical deletion of inactive user IDs, after a certain period of time?
- 15.58 Does the system demand that password length be of a minimum of 6 or 8 characters, or as the case may be, with combinations of alpha, numeric and special characters?
- 15.59 Check whether the menu options available on the web page for a customer after logging on to the system, provide only appropriate functionality as designed and that no deviation is possible.

Application Security

- 15.60 Is the security infrastructure properly tested, before using the systems and applications for normal operations? The following need to be taken care of, for ensuring that security infrastructure is tested properly, before using the systems and applications:
 - As part of the System Development Lifecycle (SDLC), during the development stage, an information security review needs to be conducted, covering the entire system and architecture review
 - Comprehensive information security-related checks need to be conducted during the coding and testing stage

- On completion of User Acceptance Testing (UAT), all Internet-related systems or applications need to be penetration tested, by an independent party
- Banks should enter into an agreement with the independent party that conducts the penetration testing, covering both, legal and contractual terms

15.61 The following should be covered, as part of penetration tests/ vulnerability tests:

1. Check for following common vulnerabilities:
 - IP spoofing
 - Buffer overflows
 - Session hijacks
 - Account spoofing
 - Frame spoofing
 - D-DOS attacks
 - Caching of web pages
 - Cross-site scripting
 - Cookie handling
2. As per RBI's guidelines, PKI (Public Key Infrastructure) is the most favoured technology for secure Internet banking services. Since the Government and RBI are in the process of identifying a PKI service provider, it may take some time to implement PKI in all the banks. However, as it is not yet commonly available, it needs to be seen if the bank uses the following alternative systems, during the transition, until the PKI is put in place:
 - A static ID and password login process.
 - Usage of SSL (Secured Socket Layer), which ensures server authentication and use of client side certificates, issued by the banks themselves, using a certificate server.
 - The use of at least 128-bit SSL for securing the browser to web server communications and, in addition, encryption of sensitive data like passwords in transit, within the enterprise itself.

Appendix B

Guidelines issued by ISACA (Information System Audit and Control Association), on areas, relevant to this book.

(Extracted from www.isaca.org with the permission of ISACA)

1. Internet banking.
2. Outsourcing of IS activities to an other organization.
3. Organization relationship and independence.
4. Effect of third-party, on an organization's IT control.
5. Application system review.

INTERNET BANKING

2.1 Definition

1. The term Internet banking, refers to the use of the Internet, as a remote delivery channel, for banking services. Services include, the traditional banking services, such as, opening an account or transferring funds to different accounts, and the new banking services, such as, electronic online payments (allowing customers to receive and pay bills through a bank's website).

2.2 Internet Banking Activities

1. More and more banks are transforming their businesses, by using Internet technology to develop or expand relationships with their customers. The extent to which the Internet is used in a bank, depends on the relative maturity of the bank with regard to Internet technology. Banks offer Internet banking in two main ways. An existing bank

with physical offices, ordinarily termed a brick and mortar bank, can establish a website and offer Internet banking to its customers, in addition to its traditional delivery channels. The alternatives available are to establish either a virtual, branchless, or Internet-only bank. The computer server or bank database that lies at the heart of a virtual bank, may be housed in an office that serves as the legal address of such a bank or at some other location. Virtual banks provide customers with the ability to make deposits and withdrawals via, Automated Teller Machines (ATMs), or through other remote delivery channels owned by other institutions. Characteristics of Internet banking include, the unprecedented speed of change, related to technological and customer service innovation, the ubiquitous and global nature of the Internet, the integration of Internet banking applications with legacy computer systems, and the increasing dependence of banks on third parties that provide the necessary Information Technology. Accordingly, a bank can perform Internet activities in one or more of the following ways:

Informational: This is the basic level of Internet banking. In this case, the bank has marketing information about the its products and services, on a stand-alone server. Risks associated with these operations are relatively low, as Information Systems typically, have no path between the server and the bank's internal network. This level of Internet banking can be provided by the bank or can be outsourced. While the risk to the bank is relatively low, the data on the server or website may be vulnerable to alteration. Appropriate controls, therefore, must be put in place, to prevent unauthorized alterations to the data, on the bank's server or website.

Communicative: This type of Internet banking system allows some interaction between the bank's systems and the customers. The interaction may be limited to electronic mail, account inquiry, loan applications, or static file updates (name and address changes). Since these servers ordinarily, have a direct path to the bank's internal networks, the operational risk is higher in the case of this configuration than with Information Systems. Controls should be in place, to prevent, monitor, and alert the management of any unauthorized attempt to access the bank's internal networks and computer systems. Virus detection and prevention controls are also important in this environment.

Transactional: This level of Internet banking allows customers to directly execute transactions that may have several financial implications.

There are two levels of transactional Internet banking, each with a different risk profile. The basic transactional site, only allows a transfer of funds between the accounts of one customer and the bank. The advanced transactional site provides a means for generating payments, directly to third parties, outside the bank. This can take the form of bill payments via, a bank official check or electronic funds transfer/automated clearing house entries. Many banks today, are also offering payments, from consumer to consumer, using either of the mentioned payment methods. When transfers of funds are allowed, to a point outside the bank, the operational risk increases. Unauthorized access in this environment can lead to or give rise to fraud. Since a communication path is usually complex and may include passing through several public servers, lines or devices, between the customer's and the bank's internal networks, this is the highest risk architecture and must therefore, have the strongest controls.

3. REVIEW OF INTERNET BANKING

3.1 Scope

1. Banking, by its very nature, is a high-risk business. The major risks associated with banking activities are: strategic, reputational, operational (including security, sometimes called transactional, and legal risks), credit, price, foreign exchange, interest rate, and liquidity. Internet banking activities have not raised risks that were not already identified in traditional banking, but it has increased and modified some of these traditional risks. The core business and the Information Technology environment are highly interlinked, thereby, influencing the overall risk profile of Internet banking. In particular, from the perspective of the IS auditor, the main issues are strategic, operational, and reputational risks, as these are directly related to, threats to reliable data flow, and are heightened by the rapid introduction and underlying technological complexity of Internet banking. Banks should have a risk management process, to enable them identify, measure, monitor, and control their technology risk exposure. Risk management of new technologies has three essential elements. Risk management is the responsibility of the board of directors and senior management. They are also responsible for developing the bank's business strategy and

establishing an effective risk management methodology. They need to possess the knowledge and skills to manage the bank's use of Internet banking and all related risks. The board should make an explicit, informed and documented strategic decision, about whether and how the bank is to provide Internet banking services. The initial decision should include the specific accountabilities, policies, and controls to address risks, including those arising in a cross-border context. The board should review, approve, and monitor Internet banking technology-related projects that have a significant effect on the bank's risk profile and ensure that adequate controls are identified, planned, and implemented.

Implementing technology, is the responsibility of the Information Technology senior management. They should have the skills to effectively evaluate Internet banking technologies and products, and to ensure that they are installed and documented appropriately. If the bank does not have the expertise to fulfil this responsibility internally, it should consider contracting a vendor who specializes in this type of business or engaging itself in an alliance, with third-party, possessing complementary technologies or expertise. Measuring and monitoring risk is the responsibility of the operational management. They should have the skills to effectively identify, measure, monitor, and control the risks that are associated with Internet banking. The board of directors should receive regular reports on the technologies employed, the risks assumed, and how those risks are being managed.

2. Internal controls over Internet banking systems should be commensurate with, the level of risk of the services the bank offers, the level of risk involved in the implementation, and the bank's risk tolerance level. The review of internal controls in the Internet banking environment, must help the IS auditor to provide a reasonable assurance that the controls are appropriate and functioning well. Control objectives for an individual bank's Internet banking technology and products, should focus on: consistency of technology-planning and strategic goals (including, effectiveness, efficiency and economy of operations, and compliance with corporate policies and legal requirements), data and service availability (including business recovery planning), data integrity (including providing for safeguarding of assets, proper authorization of transactions and reliability of the data flow), data confidentiality and privacy standards (including controls over access by both, employees and customers) and reliability of management reporting.

3. To appropriately evaluate the internal controls and their adequacy, the IS auditor should understand the bank's operational environment. COBIT 3rd Edition, published by the IT Governance Institute in 2000, has laid down seven information criteria to be met with, by the Information Systems:
 - Effectiveness
 - Efficiency
 - Confidentiality
 - Integrity
 - Availability
 - Compliance
 - Reliability
4. The information criteria listed in Section 3.1, bullet 3 of this document, are relevant in the case of Internet banking. Accordingly, a review of Internet banking should address, how the information criteria of COBIT are met with, by the Internet banking initiative/application/implementation.
5. Compared with other forms/channels of banking activities, Internet banking depends greatly, on the integrity or trust in the confidentiality of customer data and on the availability of the system. In this context, there should be in place, appropriate redundancy and fallback options, as well as disaster recovery procedures. In the case of Internet banking involving payments or funds transfers, non-repudiation and integrity of the transactions are essential attributes. In such cases, the review of Internet banking, should address the effectiveness of the Internet banking system controls, in assuring non-repudiation and integrity. Due attention should be given to them while evaluating the availability of Internet banking solutions, especially if the continuity is based on cross-border processing, because it might infringe on a regulation or might run counter to compliance with the bank's regulations.
6. It is essential in Internet banking to confirm that any communication, transaction or access request, is legitimate. Accordingly, banks should use reliable methods for verifying the identity and authorization of new customers, as well as authenticating the identity and authorization of established customers, seeking to initiate electronic transactions. Customer verification, during account origination, is important to help reduce the risk of theft, fraudulent transactions, and money laundering activities. Strong customer identification and authentication processes are particularly important in the cross-border context,

given the difficulties that may arise from conducting business electronically, with customers across national and international borders, including the risk of identity impersonation and the difficulty in conducting effective credit checks, on potential customers.

7. Auditability has great significance in the Internet banking environment, because a significant proportion of the transactions take place in paperless environments.

4. INDEPENDENCE

4.1 Professional Objectivity

1. Before accepting the engagement, the IS auditor should provide reasonable assurance that any interests he/she may have in the Internet bank under review, would not, in any manner, impair the objectivity of the review. In the event of any possible conflict of interest, these should be explicitly communicated to the bank's management and the written approval of the bank's management should be obtained, before accepting the assignment.

5. COMPETENCE

5.1 Skills and Knowledge

1. The IS auditor should have the necessary technical and operational skills and knowledge, to carry out the review of the technology employed and risks associated with Internet banking. The IS auditor should determine whether the technology and products are aligned with the bank's strategic goals. In particular, such reviews would call for knowledge of bank operations and their associated risks, knowledge of banking laws and regulations, together with the technical knowledge, necessary to evaluate aspects such as, web hosting/web housing technologies, encryption technologies, network security architecture and also security technologies, such as firewalls, intrusion detection, and virus protection. Where expert advice or expert input is necessary, appropriate use should be made of external professional resources. The fact that external expert resources may be used, should be communicated to the bank's management in writing.

6. PLANNING

6.1 High Level Risk Assessment

1. The IS auditor should gather information regarding the Internet banking objectives of the bank, the strategy used to achieve the objectives and the way that the bank is using Internet technology in its relationships with its customers (either informative, communicative, or transactional, as set out in 2.1, bullet 1). The information thus gathered, should be such that it helps in carrying out a high level assessment of the banking risks, as well as the risks pertaining to the information criteria of COBIT. This high level risk assessment will help determine the scope and coverage of the review. If the bank has an enterprise risk framework, this can be used.
2. The IS auditor should follow a risk assessment approach for analysing and evaluating the main, potential, general and specific threats, connected to the implementation of Internet banking, the possible manifestations, the potential effect on the bank, the likelihood of occurrences of risks and the possible risk management measures that can be implemented for preventing risks. The following strategic risks should be evaluated:
 - The strategic assessment and risk analysis
 - Integration within corporate strategic goals
 - Selection and management of technological infrastructure
 - Comprehensive process for managing outsourcing relationships with third-party providers
3. The following security risks should be evaluated:
 - Customer security practices
 - Authentication of customers
 - Non-repudiation and accountability of transactions
 - Segregation of duties
 - Authorization controls within the systems, databases, and applications
 - Internal or external fraud
 - Data integrity of transactions, databases, and records
 - Audit trails for transactions
 - Confidentiality of data, during transmission
 - Third-party security risk

4. The following legal risks should be evaluated:
 - Disclosure of information to customers
 - Privacy
 - Compliance with laws, rules, and statements of the regulator or supervisor
 - Exposure to foreign jurisdiction
5. The following reputational risks should be evaluated:
 - Service level delivery
 - Level of customer care
 - Business continuity and contingency planning

6.2 Scope and Objectives of the Review

1. The IS auditor should, in consultation with the bank management, wherever appropriate, clearly define the scope and objective of the review of Internet banking. The aspects to be covered by the review should be explicitly stated as part of the scope. The nature of the bank's Internet activities and volume of the Internet banking activities (set out in 2.1, bullet 1), and the risks associated with them, as identified by the high level risk assessment, dictate which aspects need to be reviewed, as well as the extent and depth of the review.
2. For the purpose of the review, control objectives should be in accordance with regulations and applicable banking laws. The Internet is borderless, so it is easy for any bank, using an Internet-based delivery channel, to operate in a multi-state and even multi-country environment. The bank may find itself bound by the laws, regulations, and customs of wherever its customers are located, rather than just where the bank is physically located. Therefore, the IS auditor should determine the geographic spread of the bank's current and planned customer base. The IS auditor needs to identify how many different jurisdictions, have legal and regulatory control over the Internet banking operations of the bank and determine how the bank is managing this.

6.3 Approach

1. The IS auditor should formulate the approach in such a way, that the scope and objectives of the review can be fulfilled in an objective and

professional manner. The approach followed, should depend on whether the review is a pre-implementation review or a post-implementation review. The approach should be appropriately documented. If the input or advice of external experts is to be used, this should be specified, as part of the approach.

6.4 Sign-Off for the Plan

1. Depending on the practices of the organization, it may be appropriate for the IS auditor to obtain the agreement of the bank's management, for the review plan and approach.

7. PERFORMANCE OF INTERNET BANKING REVIEW

7.1 Execution

1. The aspects to be reviewed and the review process, should be chosen by taking into account, the intended scope and objective of the review, as well as the approach that has been defined as part of the planning process.
2. In general, in gathering, analyzing, and interpreting the Internet banking environment, a study should be made of available documentation, such as, bank regulations about Internet banking, Internet laws, privacy laws, web banking system documentation, and use of the Internet banking solution.
3. To identify any problems relating to the Internet banking area, which have been noted previously and which may require follow-up, the IS auditor should review the following documents:
 - Previous examination reports
 - Follow-up activities
 - Work papers from previous examinations
 - Internal and external audit reports
4. The IS auditor should map the key processes, both, automated as well as manual, relating to the Internet banking initiative/system.
5. The assessment of the core business risks (set out in 6.1) should include a critical evaluation of the Internet banking objectives, strategy, and business model.
6. The IS auditor should then assess the probability that the risks identified, pertaining to these processes (business, as well as IS risks),

will materialize, together with their likely effect, and must also document the risks, along with the controls, which mitigate these risks.

7. As part of the IS risk assessment, external IS threats should be evaluated, depending on the nature of products offered by a bank and the external threats to be addressed. These threats include, Denial of Service, unauthorized access to data, unauthorized use of computer equipment, which could arise from various sources such as, casual hackers, competitors, alien governments, terrorists, or disgruntled employees.
8. Depending on the nature of the pre- or post-implementation review, the IS auditor should test the significant processes in the test and or production environment, to verify that the processes are functioning, as intended. These tests include, testing of balance inquiry, testing of bill presentation and payment, and testing the security mechanisms, using penetration testing.
9. In post-implementation review, the IS auditor should at least obtain, an understanding of network mapping, network routing, systems and network security assessment, and internal and external intrusion.
10. Since the Internet banking solution is predominantly an Information Technology solution, it should meet the information criteria, established in COBIT, as well as other relevant standards or regulations of the industry. The extent of compliance with the information criteria, standards and/or regulations and the effect of non-compliance should be analysed.

7.2 Aspects of Review

1. The following organizational aspects should be reviewed to check if:
 - Due diligence and risk analysis are performed, before the bank conducts Internet banking activities
 - Due diligence and risk analysis are performed, where cross-border activities are conducted
 - Internet banking is consistent with the bank's overall mission, strategic goals, and operating plans
 - Internet application is compliant with the defined and approved business model
 - Internet banking systems and/or services are managed in-house or are outsourced to a third-party

- The management and personnel of the organization display possession of acceptable knowledge and technical skills, to manage Internet banking
 - Measures to ensure segregation of duties, are in place
 - Management reports are adequate, to appropriately manage Internet banking transactions and payment service activities
2. The review should include policy aspects to check whether
- Suitable policies have been defined and implemented, regarding the acquisition of customers, the engagement of suppliers, the customers' authentication, the privacy of customers'/suppliers' data, audit trail, and the review of usage logs
 - The bank is keeping abreast of legal developments, associated with Internet banking
 - The bank is providing accurate privacy disclosures, associated with its Internet banking product line
 - Information is provided on the website, to allow customers to make an informed judgment about the identity and regulatory status of the bank, before they choose to make use of Internet banking services. Information to be provided, should include, the name of the bank and the location of its head office, the primary bank supervisory authority, ways to contact to customer service, and other relevant information
 - The bank, has established policies, governing the use of hypertext links, such that consumers can clearly distinguish between bank and non-bank products, and that they are informed, when leaving the bank's website
 - There are appropriate procedures in place, regarding change control, the review of audit trails and the review/analysis of usage logs (firewall logs and other reports)
 - There are suitable and adequate procedures in place, to ensure the privacy and integrity of the data and to ensure compliance with the applicable laws and regulations, as well as with best practices
3. The following planning aspects should be reviewed to check whether:
- The planned Information Systems technology architecture is feasible and will result in the safe and sound performance of operations

- There are appropriate incident response plans in place, to manage, contain, and minimize problems, arising from unexpected events, including, internal or external attacks
 - An “Internet product lifecycle” exists and if it is followed for developing, maintaining, and upgrading Internet applications
 - Business continuity and contingency plans, for critical Internet banking processing and/or delivery systems, are in place and regularly tested
4. The following Information Systems infrastructure aspects should be reviewed to check whether:
- The infrastructure and systems are capable of expansion, to accommodate the proposed business plan
 - An information security architecture has been defined and is appropriate for the nature of the Internet banking model
 - The bank has an adequate process and also controls, to address concerns about the physical security of the hardware, software, and data communications equipment, associated with the Internet banking system
 - The bank has a sound process, which ensures adequate control over the path between the website and the bank’s internal networks or computer systems and whether the internal network is suitably protected from the external, environment, using appropriate firewall technology
 - Databases and data flow are protected from unauthorized/inappropriate access
 - There are suitable and adequate procedures in place, to ensure the identification of access points and potential areas of vulnerability
 - There are appropriate manual balancing controls, where automated controls are inadequate
 - The record for each customer transaction, contains identification of the customer, the transaction number, the type of transaction, the transaction amount, and other relevant information and if it is stored and archived, for control purposes or other business functions such as, marketing
5. The following telecommunication infrastructure aspects should be reviewed to check whether:
- The network architecture is appropriate for the nature, timing, and extent of the Internet banking operation

- The network protocols used, are appropriate for the intended use (for instance, if payments or funds transfers are accepted through the Internet banking system, secure protocols should be used)
 - The bank has an effective process to assess the adequacy of physical controls that are in place, to restrict access to firewall servers and components
 - Intrusion Detection Systems and virus control systems/procedures are in place
 - There is adequate penetration testing of internal or external networks
 - The communication across the network is made secure, using Virtual Private Network (VPN) and related encryption techniques, wherever appropriate and necessary
 - Adequate and strong encryption algorithms were selected, to protect the data during communication, across the network
6. The following authentication aspects should be reviewed to check whether:
- Control features are in place, to validate the identity of prospective customers, while they use the Internet to apply for a new bank loan and/or deposit accounts
 - Control features are built into the system, to ensure the authentication of the existing customer, the integrity of data, and the confidentiality of transactions
 - Authentication procedures are used, to uniquely and positively identify the transacting party, using digital certificates and digital signatures, wherever necessary
 - Non-repudiation is ensured for an eventual, later business activity or legal use, where transactions are made using the Internet banking system
 - The fault tolerance features of the Internet banking system, are commensurate with the nature, volume and criticality of its system
7. The following third-party service provider aspects should be reviewed to check whether:
- Due diligence review of the competency and financial viability was conducted, prior to entering into any contract with third-party service providers

- The contracts with third-party service providers, adequately protect the interests of the bank and the bank's customers, and whether the bank organization has reviewed vendor contracts to ensure that the responsibilities of each party are appropriately identified and defined
 - The bank organization obtains and reviews internal or external audit reports of third-party service providers, evaluating vendor management processes or specific vendor relationships, as they relate to the Information Systems and technology, and whether all outsourced systems and operations are subject to risk management, security and privacy policies that meet the bank's own standards
 - The bank organization has the right to conduct independent reviews and/or audits of security, internal control and business continuity and contingency plans of third-party service providers
 - The security procedures of the third parties are appropriate and adequate, where the Internet banking solution depends on the any third-party service provider such as, Internet Service Providers (ISP), Certification Authority (CA), Registration Authority (RA), web-hosting/housing agency, etc.
 - Third-party service providers have appropriate business continuity and contingency plans for critical Internet banking processing, and/or delivery systems are in place, and regularly tested, and whether the bank receives copies of the test result reports
 - The bank has an adequate process to ensure that software, maintained by the vendor, is under a software escrow agreement and that the software, on a regular basis, is confirmed as being current, especially where the bank obtains software products from a vendor
 - A third party's opinion is sought, regarding in the pre-architecture solution that will be developed and configured
8. Where necessary and agreed with the bank, external expert input, or advice should be used suitably, in the collection, analysis and interpretation of the data.
 9. The inferences and recommendations should be based on an objective analysis and interpretation of the data.
 10. Appropriate audit trails should be maintained and protected for the data gathered, the analysis made and the inferences arrived at, as well as the corrective actions recommended.

11. Before finalizing the report, the observations and recommendations should be validated by the stakeholders, board of directors, and the bank's management, and declared appropriate.

8. REPORTING

8.1 Report Content

1. The IS auditor should produce regular reports on the technologies employed, the risks assumed, and how those risks are managed. Monitoring system performance is a key success factor. Depending on the scope of its coverage, the report on the Internet banking review carried out, should address the following:
 - The scope, objectives, and methodology followed and assumptions
 - An overall assessment of the Internet banking processes/systems solution, in terms of key strengths and weaknesses, as well as the likely effects of weaknesses
 - Recommendations to overcome the significant weaknesses and to improve the Internet banking processes/systems solution
 - A statement on the extent of compliance with bank regulations or applicable laws, along with the effect of any instance of non-compliance
 - A statement on the extent of compliance with the information criteria of COBIT, along with the effect of any instance of non-compliance
 - Recommendations regarding, how the lessons of the review could be used, to improve similar future solutions or initiatives

9. EFFECTIVE DATE

1. This guideline is effective for All Information System audits, beginning on or after August 1, 2003. A full glossary of the terms can be found on the ISACA website, at www.isaca.org/glossary.htm.

APPENDIX

COBIT REFERENCE

Selection of the most relevant material in COBIT, applicable to the scope of the particular audit, is based on the choice of specific COBIT IT processes and a consideration of COBIT's information criteria.

In the case of this specific audit area, viz. review of Internet banking, the processes in COBIT, likely to be the most relevant are: selected *planning and organizing* of IT processes, selected *acquisition and implementation* of IT processes, selected *delivery and support*, and *selected monitoring*. Therefore, COBIT guidance, for the following processes, should be considered relevant, when performing audit:

- PO1– Define a strategic IT plan
- PO3– Determine technological direction
- PO8– Ensure compliance with external requirements
- PO9– Assess risk
- AI2– Acquire and maintain application software
- AI3– Acquire and maintain technology infrastructure
- AI4– Develop and maintain procedures
- AI5– Install and accredit systems
- AI6– Manage changes
- DS1– Define and manage service levels
- DS2– Manage third-party services
- DS3– Manage performance and capacity
- DS4– Ensure continuous service
- DS5– Ensure systems security,
- DS8– Assist and advise customers
- DS10– Manage problems and incidents
- DS11– Manage data
- M1– Monitor the process
- M2– Assess internal control adequacy

The information criteria most relevant to an Internet banking audit are:

- *Primary*: confidentiality, integrity, availability, compliance and reliability
- *Secondary*: effectiveness and efficiency

REFERENCES

- *An Internet Banking Primer*, Federal Reserve Bank of Chicago, USA
- *Basle Directive N° 82, Risk Management Principles for Electronic Banking*, Basel Committee on Banking Supervision, May 2001, Switzerland
- *Basle Directive N° 86, Sound Practices for the Management and Supervision of Operational Risk*, Basel Committee on Banking Supervision, May 2001, Switzerland
- *Basle Directive N° 91, Risk Management Principles for Electronic Banking*, Basel Committee on Banking Supervision, July 2002, Switzerland
- *BIS Papers N° 7, Electronic finance: a new perspective and challenges*, Monetary and Economic Department, Bank for International Settlements, November 2001, Switzerland
- Cronin, Mary J., *Banking and Finance on the Internet*, John Wiley & Sons, Inc., ISBN 0-471-29219-2, USA
- Essinger, James, *The Virtual Banking Revolution*, Thomson Business Press, ISBN 1-86152-343-2, United Kingdom
- *Internet Banking Comptroller's Handbook*, Comptroller of the Currency Administrator of National Banks, October 1999, USA
- Furst, Karen, William W. Lang and Daniel E. Nolle, *Internet Banking: Developments and Prospects*, Economic and Policy Analysis
- Working Paper 2000-9, Office of the Comptroller of the Currency, September 2000, USA
- *The Internet and the National Bank Charter*, Comptroller of the Currency Administrator of National Banks, January 2001, USA
- *Treatment of material on overseas Internet world wide websites, accessible in the UK but not intended for investors in the UK*, Financial Services Authority, United Kingdom

010.010.020 OUTSOURCING OF IS ACTIVITIES TO OTHER ORGANIZATIONS

1. BACKGROUND

1.1 Linkage to Standards

1. Standard 010.010 (Responsibility, Authority, and Accountability) states, “The responsibility, authority and accountability of the Information Systems audit function, are to be appropriately documented in an audit charter or engagement letter.”
2. Standard 050.010 (Audit Planning) states, “The Information Systems auditor is to plan the Information Systems audit work, to address the audit objectives and to comply with applicable professional auditing standards.”
3. Standard 060.020 (Evidence) states, “During the course of the audit, the Information Systems auditor is to obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.”

1.2 Need for Guidelines

1. An organization (the service user) may partially or fully delegate, some or all of its IS activities, to an external provider of such services (the service provider). IS activities which can be outsourced include, IS functions such as, data centre operations, security and application system development, and maintenance.
2. The responsibility for confirming compliance with contracts, agreements, and regulations, remains with the service user.
3. The rights to audit are often unclear. The responsibility for auditing compliance is also, often not clear. The purpose of this guidelines, is to set out how the IS auditor should comply with Standards 010.010, 050.010, and 060.020, in this situation.
4. This guidelines provides guidance in applying IS auditing standards. The IS auditor should consider it, in determining how to achieve implementation of the above standards, how to use professional judgment in its application and be prepared to justify any departure from it.

2. AUDIT CHARTER

2.1 Responsibility, Authority and Accountability

1. Where any aspect of the IS function has been outsourced to a service provider, these services should be included in the scope of the audit charter.
2. The audit charter should explicitly include the right of the IS auditor to:
 - Review the agreement between the service user and the service provider (pre- or post-effect)
 - Carry out such audit work, as is considered necessary, regarding the outsourced function
 - Report findings, conclusions and recommendations to the service user management

3. PLANNING

3.1 Fact Finding

1. The IS auditor should obtain an understanding of the nature, timing, and extent of the outsourced services.
2. The IS auditor should establish what controls the service user has put in place, to address the business requirement, “to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements”. (COBIT High Level Control Objective DS2).
3. The risks associated with the outsourced services, should be identified and assessed.
4. The IS auditor should assess the extent to which, the service user’s controls provide reasonable assurance that the business objectives will be achieved, and that undesired events will be prevented, or detected and corrected.
5. The IS auditor should determine the extent to which, the outsource agreement provides for the audit of the service provider, and should consider whether this provision is adequate. This includes, assessing potential reliance on any IS audit work, carried out by either, the service provider’s internal auditors or an independent third-party, contracted by the service provider.

3.2 Planning

1. The IS auditor should consider obtaining appropriate, expert legal advice.
2. The IS auditor should evaluate any previous audit report prepared for the service provider, and plan the Information Systems audit work to address the audit objectives, relevant to the service provider's environment, taking into account the information obtained, during planning.
3. The audit objectives should be agreed upon with the service user management, before being communicated to the service provider. Any changes requested by the service provider, should be agreed upon, by the service user management.
4. The IS auditor should plan the Information Systems audit work to comply with applicable professional audit standards, as if the audit were performed in the service user's own environment.

4. PERFORMANCE OF AUDIT WORK

4.1 Audit Evidence Requirement

1. The audit should be performed, as if the service were being provided, in the service user's own IS environment.

4.2 The Agreement with the Service Provider

1. The IS auditor should consider such things as:
 - Existence of a formal agreement between the service provider and the service user
 - Inclusion of a clause in the outsourcing agreement, which explicitly states that the service provider is obligated to meet all legal requirements, applying to its activities and comply with acts and regulations, pertaining to the functions it should undertake, on behalf of the service user
 - Stipulation in the outsourcing agreement, that activities performed by the service provider are subject to controls and audits, as if they were performed by the service user itself
 - Inclusion of audit access rights, in the agreement with the service provider

614 *Information System Audit and Assurance*

- Existence of Service Level Agreements (SLAs), with performance monitoring procedures
- Adherence to the service user's security policies
- Adequacy of the service provider's fidelity insurance arrangements
- Adequacy of the service provider's personnel policies and procedures

4.3 Management of Outsourced Services

1. The IS auditor should verify that:
 - Business processes to produce the information, used to monitor compliance with the SLAs, are appropriately controlled
 - Where SLAs are not being complied with the service user has sought remedy and corrective actions have been considered, to achieve the agreed service level
 - The service user has the capacity and competence to follow up and review the services provided

4.4 Restrictions on Scope

1. Where the service provider proves unwilling to cooperate with the IS auditor, the IS auditor should report the matter to the service user's management.

5. REPORTING

5.1 Issuing and Agreeing with the Report

1. The IS auditor should provide a report, in an appropriate form, to the intended service user recipients, upon the completion of the audit work.
2. The IS auditor should consider discussing the report with the service provider, prior to its release, but the IS auditor should not be held responsible for issuing the final report to the service provider. If the service provider is to receive a copy, this should ordinarily come from the service user's management.
3. The report should specify any restrictions on distribution, which the IS auditor or service user management have agreed to impose. For example, the service provider should not be able to provide a copy of the report to other users of their service, without the permission of

the IS auditor's organization and, where appropriate, the service user. The IS auditor should also consider, including a statement, excluding liability to third parties.

5.2 Restrictions on Scope

1. The audit report should clearly identify restrictions on scope, where audit access rights are denied and should explain the effect of this restriction, with respect to the audit.

6. FOLLOW UP ACTIVITIES

6.1 Effect of Previous Audits

1. As if the audit had been performed in the service user's own environment, the IS auditor should request appropriate information from both, the service user and the service provider, about previous relevant findings, conclusions, and recommendations. The IS auditor should determine whether appropriate corrective actions have been implemented in a timely manner, by the service provider.

7. EFFECTIVE DATE

1. This guideline is effective for all Information System audits, beginning on or after 1st September 1999.

020.020.010 ORGANIZATIONAL RELATIONSHIP AND INDEPENDENCE

1. BACKGROUND

1.1 Linkage to Standards

1. Standard 020.010 (Professional Independence) states, "In all matters related to auditing, the Information Systems auditor is to be independent of the auditee, in attitude and appearance."
2. Standard 020.020 (Organizational Relationship) states, "The Information Systems Audit function is to be sufficiently independent of the area being audited, to permit objective completion of the audit."

3. Standard 030.010 (Code of Professional Ethics) states, “The Information Systems auditor is to adhere to the Code of Professional Ethics of the Information Systems Audit and Control Association.”

1.2 Need For Guidelines

1. The purpose of this guideline is to expand on the meaning of “independence”, as used in Standards 020.010 and 020.020 of the Information Systems Auditing Standards and to address the IS auditor’s attitude and independence, in Information Systems auditing.
2. This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it, in determining how to achieve implementation of the above standards, how to use professional judgment in its application and how to be prepared to justify any departure from it.

2. INDEPENDENCE

2.1 Attitude

1. IS auditors should seek to adhere to applicable codes of professional ethics and auditing standards, in all their work.
2. As per COBIT[®], the audit charter should assure that the independence, authority, and accountability of the audit function, are maintained and established by appropriate organization management.

3. PLANNING

3.1 Staffing

1. The IS auditor establishes many relationships with people involved in the audit activity and has the opportunity to explore the innermost aspects of the area that is being audited, often the whole organization. The IS auditor’s attitude should always be appropriate to this role. Planning, should take into account any known relationships.
2. IS auditors should not participate in an audit, if their independence is impaired. For example, independence is impaired if IS auditors have some expectation of financial gain or other personal advantage, due to their influence on the results of the audit. However, IS auditors’ independence would not necessarily be impaired, as a result of

performing an audit of Information Systems, where his/her personal transactions occur, in the normal course of business.

3. At the beginning of the audit, the independence of the IS auditor may be confirmed, by a signed, conflict of interest statement.

3.2 Prioritized Audit Plan

1. COBIT high level control objective M-4 states, "Management should provide for independent audit." In order to achieve this objective, an audit plan should be established. This plan should ensure that regular and independent assurance is obtained, regarding the effectiveness, efficiency, and economy of security and internal control procedures. Within this plan, the management should determine priorities, regarding obtaining independent assurance.

4. PERFORMANCE OF AUDIT WORK

4.1 Organization

1. The IS auditor should be organizationally independent of the area being audited. Independence is impaired, if the IS auditor has direct control over the area being audited. The IS auditor's independence can also be impaired if the IS auditor has direct reporting responsibility, to those individuals who have direct control over the area being audited.
2. Independence should be regularly assessed by the IS auditor and the management. This assessment should consider such factors as, changes in personal relationships, financial interests, and prior job assignments and responsibilities. The IS auditor should consider using control self-assessment techniques, in this continuous assessment process.
3. Depending on the assignment, the IS auditor can interview persons, analyse organizational processes, gain assistance from the organization's staff, etc. The IS auditor's attitude and appearance of independence, should always be adequate to meet these situations. IS auditors should be aware that the appearance of independence can be influenced by their actions or associations. Perceptions of the IS auditor's independence, could affect the acceptance of the IS auditor's work.
4. If IS auditors become aware that a situation or relationship is perceived to impair their independence, they should inform the audit management of such a perception, as soon as possible.

4.2 Gathering Information

1. Among the various items, needed to obtain an understanding of the organization that is being audited, IS auditors, in order to preserve their independence, should review:
 - Organizational policies and procedures, relating to the independent assurance process
 - Audit charter, mission statement, policies, procedures and standards, prior reports, and audit plans
 - The organizational chart

4.3 Controls Evaluation

1. The IS audit plan should define the activities, of which the IS auditor is required to be independent. The IS auditor's independence, of these activities, should be regularly monitored by the senior management, or by the person who determines and approves the IS audit plan. This monitoring should include an assessment of the process of assigning individual IS auditors to specific assignments, to ensure that this process assures independence and sufficient skills of the auditor.
2. Verification of the IS auditor's adherence to applicable professional codes of conduct should always be carried out. In many circumstances, this should be sufficient to provide audit evidence of independence. If there is an indication that the IS auditor's independence has been compromised, a revision of the audit plan should be considered.

5. REPORTING

5.1 Effect on Reporting

1. In circumstances where the IS auditor's independence is impaired and the IS auditor continues to be associated with the audit, the facts surrounding the issue of the IS should be reported.

6. EFFECTIVE DATE

1. This guideline is effective for all Information System audits, beginning on or after 1st September 2000.

050.010.040 EFFECT OF THIRD PARTIES ON AN ORGANIZATION'S IT CONTROLS

1. BACKGROUND

1.1 Linkage to ISACA Standards

1. Standard 050.010 (Audit Planning) states, "The Information Systems auditor is to plan the Information Systems audit work, to address the audit objectives, and to comply with applicable professional auditing standards."
2. Standard 060.020 (Evidence) states, "During the course of the audit, the Information Systems auditor is to obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

1.2 Definitions

1. ISP– Internet Service Provider: A third-party that provides organizations with a variety of Internet, and Internet-related services.
2. ASP/MSP– Application or Managed Service Provider: A third-party that delivers and manages applications and computer services, including security services to multiple users via the Internet or a private network.
3. BSP– Business Service Provider: An ASP that also provides outsourcing of business processes such as, payment processing, sales order processing, and application development.
4. In this guideline, ISPs, ASP/MSPs, and BSPs are collectively referred to as, third parties. Third parties covered under this guideline include any organization that is separate from the organization (such as shared service organizations), whether legally separate or not.

1.3 Guideline Application

1. When applying this guideline, the IS auditor should consider its guidance, in relation to other relevant ISACA guidelines.

1.4 Need for Guidelines

1. This guideline sets out, how the IS auditor should comply with the ISACA standards and COBIT, when assessing the effect a third-party has, on an organization's Information System controls and related control objectives.
2. This guideline is not intended to provide guidance, on how the IS auditor should report on third-party provider controls, in accordance with other standard setting entities.

2. ROLE OF THIRD-PARTY SERVICE PROVIDERS

2.1 Services of Third-party Providers

1. Organizations today, are using the Internet and corporate Intranets for a variety of purposes. These include, providing employees, vendors and customers, access to existing and/or new human resource, financial, sales, and purchasing applications. This access, in many instances, is provided through one or more third-party providers.
2. Third parties may provide such services as:
 - Connectivity of internal networks to the Internet
 - Connectivity to the organization's partners through virtual private networks or extranets
 - Connectivity to customers through the use of wireless technology
 - Website development
 - Website maintenance, management, and monitoring
 - Website security services
 - Providing physical location for hardware (known as co-location)
 - Monitoring of system and application access
 - Backup and recovery services
 - Application development, maintenance, and hosting (such as, ERP systems, E-Commerce systems)
 - Business services, including services such as, cash management, credit card, order processing, and call centre services

3. EFFECT ON CONTROLS

3.1 Third-party Provider's Effect on Controls

1. When organizations use third parties, they can become a key component in an organization's controls and in its achievement of related control objectives.
2. The IS auditor should evaluate the role that the third-party performs, in relation to the IT environment, related controls, and control objectives.
3. An organization that uses third-party providers for limited purposes, such as, co-location services, may rely upon these third parties for only limited purposes, in achieving its control objectives.
4. However, an organization that uses providers for other purposes, such as, hosting financial accounting systems and E-Commerce systems, utilizes, the third-party provider's controls, wholly, or, in conjunction with its own controls, to achieve its control objectives.
5. The effectiveness of third-party controls can enhance the ability of an organization to achieve its control objectives and conversely, ineffective third-party controls can weaken the ability of an organization to achieve its control objectives. These weaknesses can arise from many sources, including the following:
 - Gaps in the control environment, arising from the outsourcing of services to the third-party
 - Poor control design, causing controls to operate ineffectively
 - Lack of knowledge and/or inexperience of personnel, responsible for control functions
 - Over reliance on the third party's controls (when there are no compensating controls within the organization)

4. PROCEDURES TO BE PERFORMED BY THE IS AUDITOR

4.1 Obtaining an Understanding

1. As part of the planning process, the IS auditor should obtain and document an understanding of the relationship, between the services provided by the third-party and the organization's control environment. The IS auditor should consider reviewing such things as, the

contract, Service Level Agreement and policies and procedures between the third-party and the organization.

2. The IS auditor should document the third party's processes and controls that have a direct effect on the organization's processes and on its control objectives.
3. The IS auditor should identify each control, its location in the combined control environment (internal or external), the type of control, its function (preventive, detective or corrective), and the organization that performs the function (internal or external).
4. The IS auditor should assess the risks associated with the services, provided by the third-party to the organization, its controls and control objectives and should determine the significance of third-party controls in enhancing ability of the organization to meet its control objectives.

4.2 Confirming the Understanding

1. The IS auditor should confirm his/her understanding of the control environment.
2. The IS auditor can confirm his/her understanding of the control environment through a variety of methods including, inquiry and observation, and transaction walk-throughs.

4.3 Assessing the Role of Third-party Provider Controls

1. If the role or effect that the third-party has on the organization's control objectives, is significant, then the IS auditor should assess these controls to determine whether they function as desired, operate effectively, and assist the organization in achieving its control objectives.

5. RISKS ASSOCIATED WITH THIRD-PARTY PROVIDERS

5.1 Effects of Third-party Providers on an Organization

1. Third-party providers can affect an organization (including its partners), its processes, controls and control objectives, on many different levels. This includes effects arising from such things as:
 - The economic viability of the third-party provider
 - Third-party provider access to information that is transmitted through their communication systems and applications

- Systems and application availability
 - Processing integrity
 - Application development and change management processes
 - The protection of systems and information assets through backup recovery, contingency planning, and redundancy
2. The lack of controls and/or weakness in their design, operation, or effectiveness can lead to such things as:
- Loss of information confidentiality and privacy
 - Systems not being available for use, when needed
 - Unauthorized access and changes to systems, applications, or data
 - Changes to systems, applications or data that result in system or security failures, loss of data, loss of data integrity, loss of data protection, or system's unavailability
 - Loss of system resources and/or information assets
 - Increased costs incurred by the organization, as a result of any of the above

5.2 Assessing Identified Control Weaknesses

1. IS auditors should assess the likelihood (or central risk) that weaknesses in central existence, design or operation may exist in the IT environment. The IS auditor should identify, where the control weakness exists.
2. The IS auditor should then assess, whether control risk is significant and what effect it has on the control environment.
3. When weaknesses are identified, the IS auditor should also determine if compensating controls exist, to counter the effect of the identified weaknesses (compensating controls may exist in the organization, with the third-party provider or in both the entities). If compensating controls exist, the IS auditor should determine if they can help mitigate the effect of identified control weaknesses.

6. CONTRACTS WITH THIRD-PARTY PROVIDERS

6.1 Roles and Responsibilities

1. The relationship between the organization and a third-party provider, should be documented in the form of an executed contract. The

contract is a critical element in the relationship between the organization and the service provider. These contracts contain many provisions that govern the actions and responsibilities of each party.

2. The IS auditor should review the contract between the organization and the third-party.
3. Within the context of this guideline, the IS auditor should review the contract (possibly with the assistance of the organization's legal counsel), to determine the third-party's role and responsibility in assisting the organization to achieve its control objectives. Guidance on how to review a contract, is outside the scope of this guideline; however, the following list provides examples of issues that should be considered by the IS auditor, when reviewing the contract:
 - Level of service to be provided by the third-party (whether to the organization, its partners or both)
 - Reasonableness of fees charged by the third-party
 - Responsibilities for maintaining data and application privacy and confidentiality
 - Responsibilities for system, communications, operating system, utility software, data and application software access controls and administration
 - Monitoring of assets, and related data and response (organization and third-party) and reporting procedures (routine, incident)
 - Specification of ownership of information assets including, data and domain names
 - Specification of ownership of custom programming developed by the third-party provider for the organization including, change documentation, source code, and escrow agreements
 - Provision for systems and data protection including, backup and recovery, contingency planning, and redundancy
 - Right to audit clause (including, the ability to meet with the third-party provider's internal audit personnel and review their audit work papers and reports)
 - Process for negotiation, review and approval of changes to the contract and related documents (such as, Service Level Agreements and procedures)
4. As the minimum, the IS auditor should review the contract, to determine the extent of responsibility for controls that the third-party undertakes, on behalf of the organization. This process should assess

the sufficiency of identified controls and compliance monitoring/reporting, their design and operating effectiveness.

6.2 Corporate Governance

1. Even when third-party providers are involved, the management is still responsible for the achievement of related control objectives. As a part of this responsibility, the management should have a process to govern the relationship with, and the performance of, the third-party provider. The IS auditor should identify and review the components of this process. The IS auditor should review such things as, the process which the management uses to identify risks, associated with the third-party provider, the services provided by the third-party, and how the management governs the relationship between the two entities.
2. The IS auditor's review of the governance process, should ascertain such things as, whether the management reviews the third-party providers, against the performance standards or criteria, set forth in the contract and any standards specified by regulatory bodies. The governance process should include a review of such things as:
 - Financial performance of the third-party provider
 - Compliance with terms of the contract
 - Changes to the control environment, mandated by the third-party, its auditors and/or regulators
 - Results of control reviews, performed by others including, the third party's auditors, consultants or others
 - Maintaining adequate levels of insurance

7. REVIEW OF THIRD-PARTY PROVIDER CONTROLS

7.1 Contract Issues

1. When reviewing third-party provider controls, the IS auditor should consider the contractual relationship between the organization and the third-party provider and the third-party provider's evaluation and reporting on their controls.
2. Contractual issues may preclude an IS auditor from reviewing controls of the third-party provider. In these circumstances, the IS auditor should assess this limitations on his or her ability to evaluate the Information System control environment.

7.2 Independent Reports

1. Third-party providers may provide reports from independent sources, on their controls. These reports may take the form of service bureau audit reports or other control-based reports. IS auditors can use these reports as the basis for reliance on controls, in the Information System control environment.
2. If the IS auditor decides to use an independent report as the basis for reliance on Information System controls of the third-party provider, then the IS auditor should review these reports, to determine the following:
 - The independent party is qualified. For this, the auditor can check whether the independent party has an appropriate professional certification or license, has relevant experience and enjoys the confidence of applicable professional and regulatory (if applicable) authorities
 - The independent party has no relationship with the third-party provider, that would impair its independence and objectivity
 - The period of coverage of the report
 - Whether the report is sufficient, i.e. the report covers the applicable systems and controls and includes tests of areas that the IS auditor would include, had he or she performed the task work
 - If the testing of the controls is sufficient to enable the IS auditor to rely upon the work of the independent party, i.e. the testing of the controls is sufficient, as is the nature, timing and extent of the procedures performed
 - The report delineates the responsibilities of the service provider and the responsibilities of the user organization
 - The user organization has addressed its responsibilities, with respect to proper controls

7.3 Testing Third-party Controls

1. If the IS auditor decides to directly review and test controls of the third-party provider, then the IS auditor should do the following:
 - Work with the management and as applicable, or considered appropriate, internal audit of both organizations, to plan the engagement, set its objectives and scope of review

- Work with the management, and as applicable, or considered appropriate, internal audit and staff of both organizations to determine timing, staffing needs, and other issues
 - Address issues such as, access to third-party systems and assets, as well as confidentiality
 - Develop an audit programme, budget and engagement plan
 - Validate control objectives
2. Once the IS auditor has completed the fieldwork, a conclusion on the operating effectiveness of tested controls, should be made. The IS auditor should review the effectiveness of the controls within each organization and the interplay of controls between the organization and the third-party.
 3. In most situations, controls will overlap between the organization and the third-party provider. The IS auditor should assess the operating effectiveness of the controls, taken together versus considered individually.
 4. Situations may also exist, where controls for a particular objective in either organization, may not exist or do not operate effectively. In this situation, the IS auditor should assess the effect that this weakness has on the overall control environment and on the extent of their procedures.
 5. Situations may also exist, where control strengths in one organization may be partially or completely negated by the control weaknesses in another organization. The IS auditor's responsibility is to assess the effects of this situation, on the overall control environment.

7.4 Internal Auditors of the Third-party Provider

1. The IS auditor should also see if the third-party provider has an internal audit department. The presence of the third-party providers' internal auditors, can enhance the strength of the control environment at of the third-party provider.
2. If an internal audit department exists, the IS auditor should ascertain the extent of its activities, with regard to the systems and controls that effect the organization.
3. If possible, the IS auditor should review the relevant third-party provider internal audit reports.
4. In situations where it is not possible to review these reports, the IS auditor should discuss the scope of these reviews, identify what systems

and controls were covered by the reviews and the significant issues and weaknesses that the reports have identified.

5. If the third-party provider is unwilling to grant access to the reports or to their internal audit personnel, then the IS auditor should assess this restriction in context of the extent of their procedures.
6. The IS auditor should also consider assessing the skills and expertise of the third-party provider's internal audit staff. This can be accomplished through discussions with these individuals and by additional procedures such as, review of their work plans, work papers, and reports.

8. SUB-CONTRACTORS OF THIRD PARTIES

8.1 Effect on Controls

1. The IS auditor should determine whether the third-party uses sub-contractors to provide systems and services.
2. In situations where sub-contractors exist, the IS auditor should review the significance of these sub-contractors, to determine the effect they may have on the third party's primary controls that relate to the organization.

8.2 Effect on an Engagement

1. If the sub-contractor doesn't have a significant effect on the controls that are relevant to the organization, then the IS auditor should document this in his/her work papers.
2. If the sub-contractor has a significant effect on the controls that are relevant to the organization, then the IS auditor should evaluate the processes used by the third-party, to manage and monitor the relationship with the sub-contractor. The IS auditor should consider Sections 6 and 7 of this guideline, when evaluating the third party's controls over its sub-contractors.

9. REPORTING

9.1 Weaknesses

1. The IS auditor's report should indicate that the review that controls are subjected to, are extended to controls, within the organization

and also to those that exist at the third-party organization. In addition, the IS auditor should consider identifying the controls, control weaknesses, and compensating controls that exist in each organization.

2. The extent to which conclusions and recommendations are communicated, should be documented in the terms of reference. Some third parties may not be willing to, or be able to, implement recommendations. In these situations, the IS auditor should recommend compensating controls that the organization could implement, to address control weaknesses at the third-party organization.

10. EFFECTIVE DATE

1. This guideline is effective for all Information System audits, beginning on or after 1st March, 2002.

060.020.020 APPLICATION SYSTEMS REVIEW

1. BACKGROUND

1.1 Linkage to Standards

1. Standard 060.020 (Evidence) states, “During the course of the audit, the Information Systems auditor is to obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.”

1.2 Need for Guideline

1. The purpose of this guideline is to describe the recommended practices for performing an application systems review.
2. The purpose of an application systems review is to identify, document, test, and evaluate the controls over an application that are implemented by an organization to achieve relevant control objectives. These control objectives can be categorized into control objectives over the system and over the related data.

2. PLANNING

2.1 Planning Considerations

1. An integral part of planning is understanding the organization's Information System environment sufficiently, to enable the IS auditor to determine the size and complexity of the systems and the extent of the organization's dependence on Information Systems. The IS auditor should gain an understanding of the organization's mission and business objectives, the level and manner in which Information Technology and Information Systems are used to support the organization, and the risks and exposures, associated with the organization's objectives and its Information Systems. Also, an understanding of the organizational structure including, roles and responsibilities of key IS staff and the business process owner of the application system, should be obtained.
2. The primary objective of planning is to identify the application level risks. The relative level of risk, influences the level of audit evidence required.
3. Application level risks at the system and data level include such things as:
 - System availability risks, relating to the lack of system operational capability
 - System security risks, relating to unauthorized access to systems and/or data
 - System integrity risks, relating to the incomplete, inaccurate, untimely, or unauthorized processing of data
 - System maintainability risks, relating to the inability to update the system when required, in a manner that continues to provide for system availability, security, and integrity
 - Data risks, relating to its completeness, integrity, confidentiality, privacy and accuracy
4. Application controls, to address the application level risks may be in the form of, computerized controls built into the system, manually performed controls, or a combination of both. Examples include, the computerized matching of documents (purchase order, invoice and goods received report), the checking and signing of a computer-generated cheque and review by the senior management of the exception reports.

5. Where the option to place reliance on programmed controls is exercised, general relevant IT controls should be considered, as well as controls specifically relevant to the audit objective. General IT controls could be the subject of a separate review, which would include such things as: physical controls, system level security, network management, data backup, and contingency planning. Depending on the control objectives of the review, the IS auditor may not need to review general controls, such as, when an application system is evaluated for acquisition.
6. Application system reviews can be performed when a package application system is being evaluated for acquisition, before the application system goes into production (pre-implementation), and after the application system has gone into production (post-implementation). Pre-implementation application system review coverage includes, the architecture of application level security, plans for the implementation of security, the adequacy of system and user documentation, and the adequacy of actual or planned user acceptance testing. Post-implementation review coverage includes, application level security after implementation and may also cover system conversion, if there has been a transfer of data and of masterfile information, from the old to the new system.
7. The objectives and scope of an application systems review usually form part of the terms of reference. The form and content of the terms of reference may vary, but should include:
 - The objectives and scope of the review
 - IS auditor(s) performing the review
 - A statement regarding the independence of IS auditor(s) from the project
 - The time/ day of commencement of the review
 - The timeframe of the review
 - Reporting arrangements
 - Closing meeting arrangements
 - Objectives should be developed to address the 7 COBIT information criteria and then should be agreed upon, by the organization.

The 7 COBIT information criteria are as follows:

- Effectiveness
- Efficiency

- Confidentiality
 - Integrity
 - Availability
 - Compliance
 - Reliability of information
8. Where the IS auditor has previously been involved in the development, acquisition, implementation, or maintenance of an application system and has been assigned an audit engagement, the independence of the IS auditor may be impaired. The IS auditor should refer to appropriate guidelines, to deal with such circumstances.

3. PERFORMANCE OF AUDIT WORK

3.1 Documenting the Flow of Transactions

1. Information gathered should include both, the computerized and manual aspects of the system. The focus should be on data input (whether electronic or manual), processing, storage, and output that are of significance to the audit objective. The IS auditor may find, depending upon the business processes and the use of technology, that documenting the transaction flow may not be practical. In that event, the IS auditor should prepare a high level data flow diagram or narrative and/or utilize system documentation, if provided. Consideration should also be given, to documenting application interfaces with other systems.
2. The IS auditor may confirm the documentation, by performing procedures such as, a walkthrough test.

3.2 Identifying and Testing the Application System Controls

1. Specific controls to mitigate the application risks, may be identified and sufficient audit evidence obtained, to assure the IS auditor that the controls are operating, as intended. This can be accomplished through procedures such as:
 - Inquiry and observation
 - Review of documentation
 - Testing of the application system controls, where programmed controls are being tested; the use of CAATs may also be considered

2. The nature, timing and extent of testing should be based on the level of risk of the area under review and the audit objectives. In the absence of strong general IT controls, the IS auditor may make an assessment of the effect of this weakness, on the reliability of the computerized application controls.
3. If the IS auditor finds significant weaknesses in the computerized application controls, assurance should be obtained (depending on the audit objective), if possible, from the manually-performed processing controls.
4. The effectiveness of computerized controls is dependent on strong general IT controls. Therefore, if general IT controls are not reviewed, the ability to place reliance on the application controls may be severely limited and the IS auditor will be required to consider alternative procedures.

4. REPORTING

4.1 Weaknesses

1. Weaknesses identified in the application review, either due to an absence of controls or due to non-compliance, should be brought to the attention of the business process owner and to the IS management that is responsible for providing support to the application. Where weaknesses, identified during the application systems review, are considered to be significant or material, the appropriate level of management should be advised to undertake immediate corrective action.
2. Since effective computerized application controls are dependent on general IT controls, weaknesses in this area should also be reported. If general IT controls are not reviewed, this fact should be included in the report.
3. The IS auditor should include appropriate recommendations to strengthen controls, in the report.

5. EFFECTIVE DATE

1. This guideline is effective for all Information System audits, beginning on or after 1st November, 2001.

Appendix C

A MODEL INFORMATION SYSTEM AUDIT CHECKLIST

ORGANIZATION AND ADMINISTRATION

Audit Objective

Does the organization provide for adequate segregation of duties?

Audit Procedures

Review the organizational chart and the IT department's organizational chart.

S.No.		Yes/No	Comments
1.	Is there a separate IT/EDP department?		
2.	Is there a steering committee and have its duties and responsibilities, for managing MIS been clearly defined?		
3.	Has the organization developed an IT strategy with detailed long and medium-term plans?		
4.	Is the IT/EDP department independent of the user department?		
5.	Are there written job descriptions for all jobs within the IT/EDP department and have these job descriptions been communicated to the designated employees?		
6.	Are the IT/EDP personnel prohibited from having incompatible responsibilities or duties in user departments and vice versa?		

(Contd)

S.No.		Yes/No	Comments
7.	Are there written specifications for all jobs in the IT/EDP department?		
8.	Are the following functions, within the IT/EDP department, performed by separate sections:		
8.1	System design		
8.2	Application programming		
8.3	Computer operations		
8.4	Database administration		
8.5	Systems programming		
8.6	Data entry and control		
9.	Are the data processing personnel prohibited from performing duties relating to:		
9.1	Initiating transactions		
9.2	Recording of transactions		
9.3	Master file changes		
9.4	Correction of errors		
10.	Is all the processing pre-scheduled and authorized by appropriate personnel?		
11.	Are there procedures, to evaluate and establish, who has access to the data in the database?		
12.	Are the IT/EDP personnel adequately trained?		
13.	Do any of the computer operators have programming knowledge?		
14.	Are operators barred from making changes to programs and from creating or amending data before, during or after processing?		
15.	Is the custody of assets restricted to personnel outside the IT/EDP department?		
16.	Has the strategic data-processing plan been developed by the organization, for the achievement of the long-term business plan?		
17.	Are there any key personnel within the IT department, whose absence can leave the organization with limited expertise?		
18.	Are there any key personnel who are being over-relied upon?		

(Contd)

S.No.		Yes/No	Comments
19.	Is the IS/EDP audit to ensure compliance of policies and controls, established by the management, being carried out by an internal auditor or an external consultant?		

PROGRAM MAINTENANCE AND SYSTEM DEVELOPMENT

Audit Objective

Development and changes to programs are authorized, tested, and approved, prior to being placed in production.

Program Maintenance

Audit Procedures

- (i) Review details of the program library structure, and note controls which allow only authorized individuals to access each library.
- (ii) Note the procedures used, to amend programs.
- (iii) Obtain an understanding of any program library management software that is used.

S.No.		Yes/No	Comments
1.	Are there written standards for program maintenance?		
2.	Are these standards adhered to and enforced?		
3.	Are these standards reviewed regularly and have they been approved?		
4.	Are there procedures to ensure that all programs required for maintenance, are kept in a separate program test library?		
5.	Are programmers denied access to all libraries, other than the test library?		
6.	Are changes to programs initiated by written requests from the user department and have these been approved?		

(Contd)

S.No.		Yes/No	Comments
7.	Are changes initiated by the data processing department, communicated to users and approved by them?		
8.	Are there adequate controls for the transfer of programs from production into the programmer's test library?		
9.	Are all systems developed or are changes to existing system tested, according to user-approved test plans and standards?		
10.	Are tests performed for system acceptance and is the test data documented?		
11.	Are transfers from the development library to the production library carried out by persons, independent of the programmers?		
12.	Do procedures ensure that no transfer can take place, without the change having been properly tested and approved of?		
13.	Is a report, of program transfers into production, reviewed on a daily basis by a senior official, to ensure that only authorized transfers have been made?		
14.	Are all program changes properly documented?		
15.	Are all changed programs immediately backed up?		
16.	Has a copy of the previous version of the program been retained (for use, in the event of problems arising, with the amended version)?		
17.	Are there standards, for emergency changes to be made to application programs?		
18.	Are there adequate controls for program recompilation?		
19.	Are all major amendments, notified to the internal audit department for comments?		
20.	Are there adequate controls for authorization, implementation, approval and documentation of changes to operating systems?		

SYSTEM DEVELOPMENT

S.No.		Yes/No	Comments
1.	Are there formalized standards for the system development lifecycle procedure?		
2.	Do these require authorization at various stages of development, viz. feasibility study, system specification, testing, parallel running, post-implementation review, etc.?		
3.	Do the standards provide a framework for the development of controlled applications?		
4.	Are standards regularly reviewed and updated?		
5.	Does adequate system documentation exist for:		
5.1	Programmers to maintain and modify programs		
5.2	Users to satisfactorily operate the system		
5.3	Operators to run the system		
6.	Has the internal audit department been involved in the design stage, to ensure that adequate controls exist?		
7.	Testing of programs (see program maintenance.)		
8.	Procedures for authorizing new applications to production (see program maintenance.)		
9.	Are user and data-processing personnel adequately trained, to use the new applications?		
10.	Is system implementation, properly planned and implemented, by either, parallel run or pilot run?		
11.	Are differences and deficiencies observed during the implementation phase, noted and effectively resolved?		
12.	Are there adequate controls for the setting up of the standing data and opening balances?		
13.	Has a post-implementation review been carried out?		
14.	Are user manuals prepared, for all new systems and are they developed and revised for subsequent changes?		
15.	Is there a quality assurance function to verify the integrity and acceptance of the applications developed?		

PURCHASED SOFTWARE

S.No.		Yes/No	Comments
1.	Are there procedures, addressing controls for selection, testing and acceptance of packaged software?		
2.	Is adequate documentation maintained for all the software purchased?		
3.	Are vendor warranties (if any) still in force?		
4.	Is the software purchased, held in escrow?		
5.	Are backup copies of user/ operations manual kept off-site?		
6.	Are updates/ patches of the software loaded regularly and documented?		

ACCESS TO DATA FILES**Audit Objective**

Is access to data files, restricted to authorized users and programs?

ACCESS TO DATA

S.No.		Yes/No	Comments
1.	Is there any formal, written data security policy? Consider whether the policy addresses data ownership, confidentiality of information and use of password.		
2.	Is the security policy communicated to individuals in the organization?		
3.	Is physical access to offline data files, controlled in:		
3.1	Computer room/ data centre?		
3.2	Onsite library?		
3.3	Offsite library?		
4.	Does the organization employ a full-time librarian who is independent of the operators and programmers?		

(Contd)

S.No.		Yes/No	Comments
5.	Are libraries locked, during the absence of the librarian?		
6.	Are requests for online access to offline files, approved?		
7.	Are requests checked with regard to the actual files issued and initialled by the librarian?		
8.	Are sensitive applications, e.g. payroll, maintained on machines in physically restricted areas?		
9.	Are encryption techniques used, to protect against unauthorized disclosure or undetected modification of sensitive data?		
10.	Are returns followed up and non-returns investigated and adequately documented?		

COMPUTER PROCESSING

S.No.		Yes/No	Comments
11.	Does a scheduled system exist for execution of programs?		
12.	Has there been a comparison between actual and scheduled processing?		
13.	Are non-scheduled jobs approved, prior to being run?		
14.	Is the use of utility programs controlled (in particular, those that can change executable code or data)?		
15.	Are program tests restricted to copies of live files?		
16.	Is access to the computer room restricted to only authorized personnel?		
17.	Are internal and external labels used on files?		
18.	Are overrides of system checks by operators, controlled?		
19.	Are exception reports for such overrides prepared and reviewed by appropriate personnel?		
20.	Do sufficient operating instructions exist, covering the procedures to be followed during operations?		

DATABASE

S.No.		Yes/No	Comments
21.	Does the position of a Database Administrator (DBA) exist in the organization? If not, note who is responsible for:		
21.1	Defining user and program access.		
21.2	Mediating between users who share data.		
21.3	Maintaining the integrity of the database.		
21.4	Setting standards for backup and recovery.		
22.	Is the DBA restricted from:		
22.1	Having control over company assets?		
22.2	Initiating and recording transactions?		
23.	Are logs maintained, of the use of utilities, changes to access methods, etc. ?		
24.	If so, are these independently reviewed?		
25.	Does the DBMS have the facility to abort jobs when two users, with the same priority, are locked out from the same chain of data?		
26.	Are integrity checking programs run periodically, for checking the accuracy and correctness of linkages between records?		

PASSWORD AND OTHER ONLINE CONTROLS**Audit Procedures**

- (i) Note procedures for issuing, amending, and deleting passwords
- (ii) Obtain an understanding of any access control software that is used

S.No.		Yes/No	Comments
1.	Do formal procedures exist, for the issue and subsequent control of passwords?		
2.	Is there any proper password syntax in force, i.e. minimum 5 and maximum 8 characters and does it include alpha-numeric characters.		

(Contd)

642 *Information System Audit and Assurance*

S.No.		Yes/No	Comments
3.	Are there satisfactory procedures for re-issuing passwords to users who have forgotten theirs?		
4.	Are procedures in place, to ensure compliance with removal of terminated employee passwords?		
5.	Are system access compatibilities properly changed, with regard to personnel status change?		
6.	Are individual job responsibilities considered, when granting the users, access privileges?		
7.	Is each user allocated a unique password and user account?		
8.	Are there procedures in place, to ensure forced change of password after every 30 days?		
9.	Are application level security violations logged?		
10.	Do standards and procedures exist for follow up of security violations?		
11.	Do formal and documented procedures exist for use and monitoring of dialup access facility?		
12.	Are passwords made use of to restrict access to specific files?		
13.	Do terminals automatically log off, after a set period of time?		
14.	Is there a limit to the number of invalid passwords entered, before the terminal closes down?		
15.	Is there any administrative regulation, limiting physical access to terminals?		
16.	Are invalid password attempts reported to the user department managers?		
17.	Are restrictions placed on the applications that terminals can access?		
18.	Are keys, locks, cards or other physical devices used, to restrict access to only authorized users?		

APPLICATION CONTROLS

Input

Audit Objective

Do controls provide reasonable assurance that for each transaction type, input is authorized, complete and accurate, and that errors are promptly corrected?

S.No.		Yes/No	Comments
1.	Are all transactions properly authorized before being processed by computers?		
2.	Are all batches of transactions authorized?		
3.	Do controls ensure that unauthorized batches or transactions are prevented from being accepted, i.e. are they detected in time?		
4.	Is the significant standing data input, verified against the master file?		
5.	Is maximum use made of edit checking, e.g. check digits, range and feasibility checks, limit tests, etc.?		
6.	Are there procedures to ensure that all vouchers have been processed, e.g. batch totals, document counts, sequence reports, etc.?		
7.	Are there established procedures to ensure that transactions or batches are not lost, duplicated or improperly changed?		
8.	Are all errors reported, for checking and correction?		
9.	Are errors returned in to the user department for correction?		
10.	Do procedures ensure that these are re-submitted for processing?		
11.	Is an error log, maintained and reviewed, to identify recurring errors?		
12.	Are persons who are responsible for data preparation and data entry, independent of the output checking and balancing process?		
13.	Are persons who are responsible for data entry, prevented from amending the master file data?		

OUTPUT AND PROCESSING

Audit Objective

The controls provide reasonable assurance that transactions are properly processed by the computer and that the output (hard copy or other) is complete and accurate, and that calculated items have been accurately computed.

S.No.		Yes/No	Comments
1.	Is there any formal, written output distribution policy?		
2.	Are hard copy reports:		
2.1	Headed?		
2.2	Are the pages numbered?		
2.3	Dated?		
2.4	Identified by report/program number?		
2.5	Adequately totalled/control totalled?		
2.6	Designed to give an "End of Report" message, if not obvious?		
3.	Are significant reports distributed to only authorized personnel, in line with an approved distribution list?		
4.	Are there formal procedures for checking, filing and retaining reports?		
5.	Where output from one system is an input for the other, are run-to-run totals or similar checks, used to ensure no data is lost or corrupted?		
6.	Are there adequate controls forms that have monetary value?		
7.	Is maximum use made of programmed checks on limits, range's reasonableness, etc. and are items that are detected, reported for investigation?		
8.	Where calculations are 'forced', i.e. have bypassed a program check, are such items reported for investigation?		
9.	Where errors in processing are detected, is there a formal procedure in place, for reporting and investigation?		
10.	Is reconciliation between, input, output and brought forward figures, carried out and differences investigated?		

(Contd)

S.No.		Yes/No	Comments
11.	Are suspense accounts checked and cleared on a timely basis?		
12.	Are key exception reports reviewed and acted upon, on a timely basis?		

VIRUSES

S.No.		Yes/No	Comments
1.	Is there any formal written antivirus policy?		
2.	Is the policy effectively communicated to individuals in the organization?		
3.	Is there a list of approved software and suppliers?		
4.	Is only authorized software installed on microcomputers?		
5.	Is there a master library of such software?		
6.	Are directories periodically reviewed to check for suspicious files?		
7.	Are files on the system regularly checked for size changes?		
8.	Is antivirus software installed on all microcomputers?		
9.	Is antivirus software regularly updated for new virus definitions?		
10.	Are suspicious files quarantined and deleted from the terminal's hard drive and network drive?		
11.	Are diskettes formatted, before re-use?		
12.	Have procedures been developed to restrict or oversee the transfer of data between machines?		
13.	Is the staff prohibited from sharing machines?		
14.	Is the software reloaded from the master diskettes, after machine maintenance?		
15.	Has the staff been informed of the virus prevention procedures?		
16.	Are downloads from the Internet, controlled by locking the hard drive and routing them through the network drive, to prevent the virus (if any) from spreading?		

INTERNET

S.No.		Yes/No	Comments
1.	Is there any formal policy in existence, regarding the use of the Internet by the employees?		
2.	Does the policy identify the specific assets that the firewall is intended to protect and the objectives of that protection?		
3.	Does the policy support the legitimate use and flow of data and information?		
4.	Is information, passing through the firewall properly monitored?		
5.	Determine whether management approval of the policy has been sought and granted and also find out the date of the most recent review of the policy, by the management.		
6.	Has the policy been properly communicated to the users and has awareness regarding this, been maintained?		
7.	Has the company employed a firewall administrator?		
8.	Is the firewall configured, as per the security policy?		
9.	Is URL screening being performed by the firewall?		
10.	Is antivirus inspection, enabled?		
11.	Are packets screened, for the presence of prohibited words? If so, determine how the list of words is administered and maintained.		
12.	Are access logs regularly reviewed and is any action taken on questionable entries?		

CONTINUITY OF OPERATIONS**(a) Physical Protection****1. Fire Hazard**

S.No.		Yes/No	Comments
1.	Fire resistance:		
1.1	Are building materials fire-resistant?		

(Contd)

S.No.		Yes/No	Comments
1.2	Are wall and floor coverings non-combustible?		
1.3	Is there separation from hazardous areas (e.g. fire doors)?		
1.4	Is there separation from combustible materials (e.g. paper, fuel)?		
1.5	Are there smoking restrictions?		
1.6	Are there fire-resistant safes (for tapes, disks and documentation)?		
2.	Fire-detection:		
2.1	Are there smoke/heat-rise detectors?		
2.2	Are the detectors located on the ceiling and under the floor?		
2.3	Are the detectors located in all key EDP areas?		
2.4	Are they linked to the fire alarm system?		
3.	Fire-extinction:		
3.1	Is there a halon gas system (for key EDP areas)?		
3.2	Is there an automatic sprinkler system?		
3.3	Are there portable CO ₂ extinguishers (electrical fires)?		
3.4	Is there ease of access for fire services?		
4.	Fire emergency:		
4.1	Are fire instructions, clearly posted?		
4.2	Are fire alarm buttons, clearly visible?		
4.3	Have emergency power-off procedures been posted?		
4.4	Is an evacuation plan, with assignment of responsibilities in place?		
5.	Fire practices:		
5.1	Does the organization conduct regular fire drill and training?		
5.2	Is there regular inspection/testing of all equipment?		

2. Water Damage

S.No.		Yes/No	Comments
1.	Is the EDP area, located above ground level?		
2.	Is the building, weather-protected (e.g. against storms, water leaks)		
3.	Are there computer room drainage facilities?		

3. Air-conditioning

S.No.		Yes/No	Comments
1.	Is there monitoring of temperature and humidity in the EDP area?		
2.	Is there heat, fire and access protection, of sensitive air conditioning parts (e.g. cooling tower)?		
3.	Are any air intakes located, to avoid undesirable pollution?		
4.	Is there any air-conditioning backup equipment?		

4. Power Supply

S.No.		Yes/No	Comments
1.	Is there a reliable local power supply?		
2.	Is there provision for a separate computer power supply?		
3.	Is the line voltage monitored?		
4.	Is the power supply regulated (for voltage fluctuation)?		
5.	Is uninterrupted power supply (e.g. battery system) available?		
6.	Are there any arrangements for alternative power supply (e.g. generator)?		
7.	Is there an emergency lighting system?		

5. Communications Network

S.No.		Yes/No	Comments
1.	Is there a mechanism to ensure the physical protection of communication lines, modems, multiplexers and processors?		
2.	Is the location of the communication equipment, separate from the main EDP equipment?		
3.	Are there backup and dialup lines for direct lines?		

6. Machine Room Layout

S.No.		Yes/No	Comments
1.	Are printers, plotters located in separate areas?		
2.	Is the printout preparation (e.g. bursting), located in a separate area?		
3.	Is tape/ disk library in a separate area? Is the machine room kept tidy?		
4.	Are security devices located in practically feasible areas?		
5.	Are there emergency power-off switches?		
6.	Are there alarms?		
7.	Are there extinguishers?		
8.	Is environment monitoring equipment available?		

(b) Access Control**1. Entrance Routes (EDP areas)**

S.No.		Yes/No	Comments
1.	Are there unnecessary entrances to the computer room?		
2.	Are unessential doors, always shut and locked, on the outside? (e.g. fire exits)		
3.	Are air vents and daylight access locations protected?		
4.	Is the use of all open doors controlled?		

2. Access Control

S.No.		Yes/No	Comments
1.	Is access restricted to selected employees?		
2.	Is prior approval required by all other employees?		
3.	Is the entrance door controlled by:		
3.1	Screening by a guard?		
3.2	Locks/ combinations?		
3.3	Electronic badge/ key?		
3.4	Others (specify)		
4.	Is there a system of positive identification of all employees, e.g. identification card?		
5.	Are all unknown personnel challenged?		
6.	Is verification of all the items that are taken into and out of the computer room carried out?		
7.	Is access, controlled on a 24 hours basis, including weekends (e.g. automatic control mechanism)?		
8.	Are locks, combinations, badge codes, changed periodically?		
9.	Is access to copies of the documentation, kept in a secure location?		

3. Visitor Control

S.No.		Yes/No	Comments
1.	Is positive identification always required?		
2.	Are temporary badges issued, controlled and returned on departure?		
3.	Are all visitors and visits logged in and out?		
4.	Are visitors accompanied and observed at all times?		

4. Terminal Security

S.No.		Yes/No	Comments
1.	Are all terminals located in secure areas?		
2.	Are alarm systems used, to control microcomputers from being disconnected or moved from their assigned location?		
3.	Are sensitive applications, e.g. payroll, maintained on machines in physically restricted areas?		
4.	Are terminal keys/locks used?		
5.	Are passwords changed regularly?		
6.	Are identification labels placed on each terminal?		

5. General Security

S.No.		Yes/No	Comments
1.	Is waste regularly removed from the EDP area and sensitive data shredded?		
2.	Is there a window and door alarm system?		
3.	Is there closed circuit television monitoring?		

(c) Personnel Policies

S.No.		Yes/No	Comments
1.	Are new employees, recruited according to job description and job specification?		
2.	Are employee identity cards issued?		
3.	Are performance evaluation and regular counselling conducted?		
4.	Is there a continuing education program?		
5.	Is training in security, privacy and recovery procedures imparted?		
6.	Are all functions covered by cross training?		

(Contd)

652 *Information System Audit and Assurance*

S.No.		Yes/No	Comments
7.	Are critical jobs rotated periodically (e.g. operators, program maintenance)?		
8.	Has a clean desk policy been enforced?		
9.	Is there fidelity insurance for key personnel?		
10.	Are contract service personnel vetted (e.g. cleaners)?		

(d) Insurance

S.No.		Yes/No	Comments
1.	Does adequate insurance exist to cover:		
1.1	Equipment?		
1.2	Software and documentation?		
1.3	Storage media?		
1.4	Replacement/ re-creation cost?		
1.5	Loss of data/ assets (e.g. accounts receivable)?		
1.6	Business loss or interruption (business critical systems)?		
2.	Is adequate consideration given, to cover additional cost of working and consequential losses?		

(e) Backup Procedures**1. Equipment (Computer and Ancillary)**

S.No.		Yes/No	Comments
1.	Is regular preventive, maintenance undertaken?		
2.	Is the manufacturer, service-reliable?		
3.	Is there any arrangement for backup installation?		
4.	Are formal written agreements in place?		
5.	Is compatibility regularly checked?		
6.	Is sufficient computer time available, at backup?		
7.	Is testing of the backup regularly performed?		

2. Outside Suppliers (Non-continuance/Disaster)

S.No.		Yes/No	Comments
1.	Are alternative sources of supply/maintenance/service available?		
2.	Are adequate and secure documentation/backup of data and programs available?		
3.	Are backup copies of system documentation kept in a secure location?		

3. Offsite Storage

S.No.		Yes/No	Comments
1.	Secure separate location		
2.	Is there adequate physical protection (see Section A)?		
3.	Is a log for of offsite materials maintained?		
4.	Is the offsite inventory regularly reviewed?		
5.	Is file transportation undertaken with adequate physical protection?		
6.	Are backup files periodically tested?		

4. Data Files

S.No.		Yes/No	Comments
1.	Are file criticality and retention procedure, regularly reviewed?		
2.	Have at least three generations of important tape files been retained?		
3.	Are copies of all the updating transactions, for the above, retained?		
4.	Is at least one generation and all necessary updating transactions in offsite storage?		
5.	Have checkpoint/ restart procedures been provided for?		

(Contd)

654 *Information System Audit and Assurance*

<i>S.No.</i>		<i>Yes/No</i>	<i>Comments</i>
6.	Is audit trail (log file) of transactions, updating online files (database), maintained?		
7.	Are regular tape dumps of all disc files, stored offsite?		
8.	Is the audit trail (log file) regularly dumped and stored offsite?		

5. Software

<i>S.No.</i>		<i>Yes/No</i>	<i>Comments</i>
1.	Are copies of the following, maintained at offsite storage:		
1.1	Production application programs?		
1.2	Major programs under development?		
1.3	System and program documentation?		
1.4	Operating procedures?		
1.5	Operation and system software?		
2.	Are all copies regularly updated?		
3.	Are backup copies regularly tested?		

6. Operations

<i>S.No.</i>		<i>Yes/No</i>	<i>Comments</i>
1.	Is the backup procedure manual available?		
2.	Are there priority assignments for all applications?		
3.	Are procedures for restoring data files and software available?		
4.	Are procedures available for backup installation?		

7. Disaster Recovery Plans

S.No.		Yes/No	Comments
1.	Has a comprehensive contingency plan been developed and documented and is it periodically tested to ensure continuity in data-processing services?		
2.	Does the contingency plan provide for recovery and extended processing of critical applications in the event of a catastrophic disaster?		
3.	Has any Business Impact Analysis been carried out by the company?		
4.	Are all recovery plans approved of and tested, to ensure their adequacy in the event of a disaster?		
5.	Has it been communicated to all the levels of management and other concerned personnel?		
6.	Have critical processing priorities been identified? (e.g. significant accounting applications)		
7.	Have disaster recovery teams been established to support the Disaster Recovery Plan?		
8.	Are responsibilities of individuals, within the disaster recovery team defined and has time been allocated for completion of their tasks?		
9.	Are there operation procedures for the use of equipment and software backup?		
10.	Has the company developed and implemented adequate plan maintenance procedures?		
11.	Are priorities set for the development of critical systems?		
12.	Does a hardware maintenance contract, with a reputed supplier exist?		
13.	Does the recovery plan ensure that, in the event of failure: - There will be no loss of the data received, but not processed - There will be no re-processing of data, already processed - Files not corrupted by partially-completed processing		
14.	Are recovery plans regularly tested?		

This checklist is basically designed for a general audit exercise that would indicate the strong and weak points of the organization. Based on this, specialized audit, viz. Intranet audit, audit of the business continuity operations, etc. can be conducted.

REFERENCES AND SUGGESTED READING

BOOKS

1. Weber Ron—*Information System Control and Audit*, Pearson Education 2002 reprint.
2. Martin A. Krist— *Standard for Auditing Computer Application*, Aurebach.
3. Alvin A. Arens and James K. Loebbecke— *Auditing—An Integrated Approach*, Prentice Hall International— Eighth Edition.
4. Rittenberg and Schwieger— *Auditing (Fourth Edition) —Concepts for a Changing World*, Thomson-South Western.
5. Federick Gallegos, Daniel P. Manson, Sandra Allen-Senft— *Information Technology Control and Audit*, Aurebach.
6. James A. Hall— *Information System Auditing and Assurance*, South-Western College Publishing.
7. Bhatia Mohan— *Auditing in a Computerized Environment*, Tata McGraw-Hill, India.
8. Donn B. Parker— *Fighting Computer Crime—A New Framework for Protecting Information*, John Wiley and Sons Inc.
9. Andref Blyth and Gerald Kovacich— *Information Assurance—Surviving in the Information Environment*, Springer.
10. Andrew Hiles— *Enterprise Risk Assessment and Business Impact Analysis Best Practices*, ISBN.
11. Mark B. Desman— *Building Information Security Awareness Program*, Aurebach.
12. Sanjiv Singhal— *Internet Banking The Second Wave*, Tata McGraw-Hill, India.
13. Dimitris N. Chorafas— *Operational Risk Control with Basel II*, Elsevier Butterworth, Heinemann.
14. *Advances in Operational Risk Firm wide Issues for Financial Institution*, Published in association with SAS Second Edition.

15. Abraham Silverschatz and Peter Baer Galvin– *Operating System Concepts*, AWL International students Edition.
16. Gordon E. Smith– *Network Auditing—A Controls Assessment Approach*, John Wiley and Sons Inc.
17. Erik Schetina, Ken Green and Jacob Carlson– *Internet Site Security*, Addison-wesley.
18. Sundeep Oberoi– *E-Security and You*, Tata McGraw-Hill, India.

REPORTS AND OTHER PUBLICATIONS

19. *Information System Audit Policy for the Banking and Financial Sector*, Reserve bank of India 2001.
20. *Preventive Vigilance Manual for Computerized Branches of Banks*, Published by Indian Banks Association.
21. *Control Objectives for Information and Related Technology (COBIT)*, Third Edition ISACA (USA).
22. *Control Objectives for Net Centric Technology (CONCT)*, ISACA (USA).
23. *CISA Review Manual*, 2002/ 2003.

WEBSITES

1. <http://www.isaca.org/> (Information Systems Audit and Control Association)
2. www.rbi.org.in (Reserve Bank of India)
3. www.nist.gov (National Institute of Standard and Technology)
4. <http://www.acl.com/audit.html> (Audit Central)
5. <http://www.aol.com/auditnet/karlhome.html> (Jim Kaplan's listing of websites for auditors)
6. <http://www.auditserve.com/> (Technical Research Center for Control Professionals)
7. <http://www.bitwise.net/iawww/> (Internal audit web page)
8. <http://www.rutgers.edu/Accounting/raw/iia> (Institute of Internal Auditors)
9. <http://www.misti.com/> (MIS Training Institute)
10. http://www.netaxs.com/~edoig/ASAP_index.html (publicly-shared audit programs)
11. <http://www.tc.pw.com/tc/217e.htm> (Price Waterhouse Expert Assistance for Audit Planning).

Index

A

- Acceptance certificate 553
- Acceptance testing 552
- Access control 180, 394, 471
- Access Control List (ACL) 273, 276, 277, 315
- Access rights 385
- Account lockout 410
- Account spoofing 593
- Accountability 70, 72, 73
- Accounting audit trail 190
- ACID property 218
- ACK bit NOT set 366
- ACK bit set 366
- ACL 54, 56, 57, 315, 367
- Active content 313
- ActiveX 314, 316, 363
- AH (Authentication Header) 267
- AICPA 2, 41, 145
- Air-conditioning 467
- AIT 515
- ALPM 173
- Alternative routing 509
- AMC 444
- Annual backup 433
- Anti-virus software 30, 36
- Antivirus 286, 442, 546
- AOF 424, 452, 469, 486
- API 315
- Applets 314
- Application control 219
- Application level firewall 274
- Application proxy firewall 275
- Application server 309
- Application system 31, 171
- Archiving 430
- ARPANET 310
- ASCII 196, 382
- ASIC (Application Specific Integrated Circuits) 273
- ASP 309
- ASP files 359
- Asset classification 285
- Assets 82
- Assurance 3, 4, 5, 108, 209
- Assurance services 2
- Asymmetric crypto system 333
- Asynchronous replication 496, 516
- ATM 109, 119, 142, 148, 191, 281, 439, 526, 570
- ATM network 367
- Atomicity 218
- Attestation services 6, 18
- Attribute sampling 48
- Audimation 55
- Audit approaches 79
- Audit charter 69, 72, 103, 280
- Audit Hook (AH) 51, 63
- Audit leverage 55
- Audit methodology 79
- Audit planning 77, 81
- Audit policy 411
- Audit trail 189, 200, 206, 211, 226, 235, 394, 556, 578
- Auditing around the computer 80
- Auditing through the Computer 80
- Auditing with the Computer 80
- Authentic 180
- Authentication 185, 333, 446, 573

660 *Index*

authenticity 115, 421, 423
Authenticode 317
Authority 70, 72, 74
Authorization controls 569
Auto audit 2001 55
Autoexec.Bat 188
Automated audit services 55
Automated Operations Facility (AOF)
423, 424, 439, 479, 484
Automated Teller Machines (ATMs)
174
Automated vulnerability scanning tool
90
availability 32, 95, 452

B

Backup 286, 420, 422, 424–427,
429, 433, 443, 480–481, 523, 553
Backup techniques 434
Backups 430
Banks' website 318
Banyan vines 384
Base Case System Evaluation (BCSE)
220
Basel Committee 473
Basel II 475, 485
Basic Indicator Approach (BIA) 475
Basle Committee 58, 61
Bastion host 272
Batch control 194
Batch tickets 195
BCP 491, 494, 512, 514, 535
BCP process 494
BCP strategy 499
BCP-DRP 492, 498, 528
Before and after image processing
205
Behaviour-based IDS 279
BIA 495, 497, 498, 500, 503, 520
Binary object code 314
Biometric control 38

Biometric system 184
BIOS 399, 402, 404, 407
Blackmail 87
Block ticket 195
BOD (beginning of day) 523
Border Gateway Protocol (BGP) 313,
526
Bottom-up 128
Boundary 179
Boundary control 225, 229
Bridge 255, 282
British standard 7799 107
Broadcast domain 259
Broadcast IP 265
Browser 177, 308
BS7799 42
Btrieve files 224
Buffer overflows 593
Bugs 553
Bulk erasers 453
Bus 383
Bus topology 250
Business continuity planning 491
Business Impact Analysis (BIA) 94,
494, 520, 535, 536
Business Process Re-engineering (BPR)
12, 544
Business strategy 543
Byte code 314

C

C++ 313
CA 339
CAAT 51, 103
CAATT 49, 50, 52, 53, 54, 55, 56,
57, 65, 80
Cable 253, 256
Calculated fields 225, 228
Campus Area Network (CAN) 247
Cash infusion 139
Cataloguing 281

- CD-ROM 362, 413
- Central Banking Solutions (CBS) 147
- Centralized 78
- CERT 349
- Certificate Policy Statement (CPS) 337
- Certificate Revocation List (CRL) 337
- Certified Information System Auditor (CISA) 18, 103
- Certified Information Systems Security Professional 103
- Certified Public Accountants (CPAs) 5, 57
- CGI 359
- CGI script 371
- Challans 172
- Change management 287
- Change Request Form (CRF) 580, 582
- Chargeback 461, 462
- Charged pipe 468
- Charter 79, 102
- Check sum 228
- Checklist 93, 157, 172, 399, 400, 406, 543, 551
- Checkpoint/restart 207, 211
- Cheques 172
- CISA 11, 12, 74, 102
- CISA/CISSP 23
- CISMTM 11
- CISSP 102
- Class 261
- Classful 266
- Classless 266
- Clean desktop 287
- Clearing 172, 439
- Clearing House Automated Payments System (CHAPS) 500
- Client server application 174
- Client-server 247
- Closed User Group (CUG) 321
- Clustered banking 122
- CO₂ 469
- COBIT 9, 14, 15, 19, 30, 32, 33, 42, 100, 107, 113, 127, 155, 212, 239, 472
- COBOL 22, 189, 196, 224
- Coercivity 451
- Cold backup 438
- Cold site 504, 537
- Collision domain 259
- Collisions 259
- Common Gateway Interface (CGI) 354
- Compensatory control 38, 61, 573
- Compliance 32
- Compression 255
- Concurrency 189
- Confidential 132, 443
- Confidential agreement 132
- Confidentiality 32, 84, 95, 115, 333, 452
- Conflict of interest policies 134
- Consistency 218
- Consolidation 7
- Consumables 448, 480
- Content control 209
- Contingency planning 547
- Control 7, 28, 30, 39, 92, 93, 99, 145, 152, 271
- Control risk 41, 42
- Control totals 195, 196, 202, 204, 228
- Controlling 115, 151, 163
- Controls 93, 124
- Conversion audit 224
- Cookies 314, 330, 593
- Cooperative process management 379
- Core banking 118, 122, 570
- Core banking solution 39
- Core competency 141

662 *Index*

Corrective 61
Corrective control 37
COSO 32, 57, 58
CP/M 379
CPU 393, 425
Critical Success Factor (CSF) 152, 153
Criticality 94
Cross footing 206
Cross-site scripting 593
Cross-training 135
Cryptography 575
CSF 166
CSMA/CD 250
CTRL+ALT+DEL 413
CUG (Closed User Group) 320, 322, 323, 325, 326, 327, 522
Cut through switch 259

D

D-DOS attacks 593
DARPA 310
Dashboard 461
DAT 515
Data center 319, 342
Data conversion 556
Data integrity 9, 216, 225, 569
Data migration 552
Data replication 516
Data storage 518
Data-entry screen 197
Database 105, 309, 320, 342, 428, 443, 590
Database administration 426
Database Administrator (DBA) 67, 167, 344
Database management 179
Database Management System (DBMS) 217, 225, 239, 315, 372, 436, 437, 486
DBA 68, 436
De-militarized zone 589

Default gateway 266
Degaussing 453
Demon dialer 291
Demonstration effect 152
Denial of Service (DOS) 305, 380, 525, 587
Denial-of-Service Attack (DoS Attack) 270
Dense Wavelength Division Multiplexing (DWDM) 518
Desired output 28
Desktop systems 376
Detection risks 41, 42
Detective 61
Detective control 36, 37
Dictionary-based attack 268
Difference estimation 49
Digital signature 182, 210, 333
Digital Subscriber Loop (DSL) 372
Direct access file backup 435
Direct Memory Access (DMA) 387
Directory structures 382
Disaster 104, 427
Disaster recovery 553
Disaster recovery planning 491, 546
Disclosing 134
Disclosure 115
Discovery sampling 48
Disruptive technology 120
Distributed 78
Distributed Denial of Service (DDOS) 87, 305
Distributed Denial-of-Service Attack (DDoS Attack) 270
Distributed systems 376
Diverse routing 509
DLT 515
DMZ 320, 331, 367
Domain 385, 394, 442
Domain controller 409, 413
Domain integrity 217
Dotcom 307

Downtime 425
Downtime register 461
DRP 491, 494, 556
DRP (Disaster Recovery Plan) 535
DTF 515
Dumb terminal 176
Dump 437
Duplicate Information Processing Facility (DIPF) 504
Duplicate processing facility 537
Durability 218
DVD 515
Dynamic 28, 29, 141

E

E-Commerce 5, 169
E-mail 160, 313, 318, 419, 546, 576
EAM 63
Edit controls 220
EDP manager 64
EEPROM 183
Effectiveness 9, 32
Efficiency 10, 32
Electronic Data Processing (EDP) 6
Electronic Funds Transfer (EFT) 537
Embedded Audit Module (EAM) 50, 222, 242
Embedded operating systems 378
Embedded systems 376
Employee handbook 136
Enable password 277
Encode 172
Encoding 195
Encryption 182, 255
Engagement letter 69, 71, 79, 103, 280
Entity integrity 217
Entropy 463
EOD (End of Day) 523
Error detection service 393
Escrow mechanism 551

ESP (Encapsulated Security Payload) 267
Event log 206, 414
Evidence 43, 44
Exception reporting 556
Existence control 190, 201, 206, 211
Export 437
EXT2/EXT3 390
Extinguishers 478

F

Facilities 31
Factoring 213, 214
FAT 390
FCIP 518
Fiduciary 31, 32
File management 380
File System (FS) 380
File Transfer Protocol (FTP) 90, 255, 315, 360–363
Fire extinguisher 469
Fire protection 478
Fire suppression 468
Fire-detection system 471
Firewall 29, 88, 272, 277, 282, 313, 330, 331, 369, 408, 422, 556, 589
Fish bone 459
Floppies 452
Floppy-based Input Clearing (FBIC) 489
FM-200 468
Foreign key 217
Format control 210
Four blockers 459
Frame spoofing 593
Framework 118
Fraud 87
Frequency estimating sampling 48
Fully operational test 512

664 *Index*

Fully transactional websites 318
Fully-qualified domain name 338

G

Galileo 55
Generalized Audit Software (GAS) 50
Generation number 196
GET/POST operations 355
Grandparent-Parent-Child (GPC) 434
Graphical User Interface (GUI) 391
GUI features 387

H

Hackers 88
Hardening 400
Hardening procedure 284
Hardening the OS 397
Hardware 374, 421, 422, 425, 426, 442, 455
Hardware Security Module (HSM) 335
Hash 195, 196, 441
Hash function 333
Hash total 569, 572
Hazards 474
Help desk 142, 422, 454, 482, 583
Hidden fields 330
Hiring 130
Hits 459
Host-based IDS (HIDS) 278
Hot backup 438
Hot site 503–504
HPFS 390
HSM 336
HTML 310, 313, 371
HTTP 310, 314, 315, 359, 360
Hub 258, 282
Hyper Text Markup Language (HTML) 308

I

I-key 335, 336
IANA (Internet Number Assigning Authority) 264
IB (Internet Banking) 320
IDEA 54
Identification 185
IDRBT 18, 337
IDS (Intrusion Detection System) 278, 320, 331, 369, 406
IETF (Internet Engineering Task Force) 267
iFCP (Internet Fibre Channel Protocol) 518
IIS (Internet Information Server) 308
Impact analysis 94, 113
Import 437
Incident handling 286
Incident management 352
Independence 73
Independent 2, 102, 116
Indian Financial Network (INFINET) 320, 321, 522
Inference control 207
Information Security Administrator (ISA) 577
Information security officer 547
Information system 146
Inherent risk 41, 215, 216
Input 28, 29, 179
Input control 232, 565
Input subsystem 191
Input/output control 482
Insecure settings 284
Insourcing 544
Installation 399
Insurance 503
Integrated Test Facility (ITF) 51, 221, 242
Integrity 32, 84, 95, 115, 333, 424, 448, 452

Inter Branch Reconciliation (IBR) 195
 Interface controls 568
 Interference 115
 Internal level 196
 Internal measurement approach 475
 International Standard Organization (ISO) 110
 Internet 3, 264, 307, 310, 311, 464
 Internet banking 281, 307, 348, 570, 586
 Internet Banking Application Server (IBAS) 341, 342
 Internet Banking DB Server (IBDS) 341
 Internet banking system 207
 Internet Engineering Task Force (IETF) 263
 Internet explorer 314
 Internet Protocol (IP) 261
 Internet Service Provider (ISP) 264, 311, 313, 371, 522, 525, 526
 Interrupt Requests (IRQs) 387
 Intrusion Detection System (IDS) 278, 313, 368, 588
 Intrusion detection tools 88
 Intrusion-detection 351
 Inventory 444
 IOS 367
 IP 255
 IP address 261, 442
 IP forwarding (routing) 364
 IP network 260
 IP spoofing 269, 593
 IPv6 267
 IPX 255
 ISA 578
 ISACA 11, 12, 38, 75, 100
 ISAPI 358
 Ishikawa 459
 ISO 554
 ISO17799 107

Isolation 218
 IT Act, 2000 337
 IT plans 126, 159
 IT security policy 563, 589

J

Java 313, 316, 317
 Java beans 316
 Java virtual machine 317
 Job schedule 441
 Judgmental sampling 47
 Just-in-time compilers 314

K

Key Goal Indicator (KGI) 152, 153, 166
 Key Performance Indicator (KPI) 152, 154, 166, 458
 Keystroke dynamics 183

L

LAN 160, 216, 320, 343, 392, 413, 464, 518, 546
 Latency 321, 323
 Leading 115, 149, 162
 Librarian 442, 447, 451
 Library 447
 Licenses 426
 Licensing agreement 446
 Licensing requirements 560
 Light out facility 484
 Light-out 423, 424
 Likelihood 93, 97
 LILO/GRUB 407
 Limit check 192, 243
 Linux 378, 379, 384, 388, 389, 393, 406, 416
 Linuxconf 408
 Local Area Network (LAN) 246, 447, 486
 Log 286, 438

666 *Index*

Log parsers 287
Logging 394, 443
Logical topology 249
Login scripts 188
Logon ID 180
Logs 426
Long-range IT plans 545
Long-range plans 116
Long-term plan 544
Longevity 449
Loop-back testing 264
Losses 82

M

Magique 55
Main memory management 380
Mainframe system 375
MAN 160, 546
Man-in-the-Middle Attack 270
Management controls 84
Manuals 426
Mapping 219
Master data 226
Master reference 193
Materiality 41
MD5 334
Mean Time Before Failure (MTBF) 450
Media Access Control (MAC) 259, 261
Medium control 210
Messenger 362
Methods 144
Metric 260
Metropolitan Area Network (MAN) 247
MICR 191
Microsoft Exchange 2000 419
Mid-process data correction 204
Middleware 309, 319, 321–326, 342
Mime types 381

MIS 423
Misrepresentation 115
Monthly backup 432
Montreal protocol 468
Motivation 86, 87
MS DOS 379, 389, 392
MS Windows 391
Multi-layered concept 319
Multi-layered security 329
Multi-processing 377, 379
Multi-user application 173
Multi-user operating systems 378
Multiplexing 255
Mummification 492

N

Navigation control 187
NetBIOS 364, 388
Network 105, 246, 401, 403
Network administrators 343, 426
Network Attached Storage (NAS) 519
Network cabling 256
Network communication 392
Network File System (NFS) 388
Network Interface Card (NIC) 261
Network IP 265
Network management 384, 573
Network-based IDS (NIDS) 278
NFS 364
NIC 255, 267
NIS 364
NIST 83
Non-compete agreement 134
Non-disclosure agreement 133, 462, 465
Non-Performing Assets (NPA) 146
Non-repudiation 333
Novell Netware 4 66, 384
NTFS 364, 390, 409, 412
NTLMv2 413

O

Object Linking and Embedding (OLE) 314, 316
 Object Model (COM) 314
 Obsolescence 449, 450
 OCR 191
 Oersteds 451
 OLTP 173, 194
 Operating Costs 137
 Operating System (OS) 374, 375, 426, 562
 Operational audit trail 189, 211
 Operational controls 84
 Operational risk 13, 473, 475
 Operational Risk Management (ORM) 473, 488
 Optical fibre 258
 Organizing 115, 127, 159
 ORM 474
 OSI 254, 259, 260, 261, 274, 392
 Output 29, 179
 Output control 207, 210, 237, 568
 Outsource vendors 143
 Outsourcing 136, 140, 352, 421, 454, 544, 556

P

Packet 255
 Packet filter firewall 275
 Packet filtering 273
 Packet sniffing 267
 Paper test 512
 Parallel Simulation (PS) 51
 Parking accounts 226
 Password 180, 182, 396, 400, 404, 410, 413, 426, 574
 Password attacks 268
 Password policy 410
 Patch management 287
 PDC (Primary Domain Controller) 419

Penetration testing 90, 91, 344, 547, 579
 Pentana 55
 Perimeter security 272
 Perl 309
 Personal Identification Numbers (PINs) 175, 183, 574
 Perturbation control 208, 209
 Pervasion 7
 Phishing 337
 Physical topology 249
 Ping 270
 Planning 77, 115, 125, 126, 157
 Policies 128, 166
 Population standard deviation 47
 Port 258
 Port scanning 269
 POS 191
 Positive Balance File (PBF) 439, 521
 Post-installation 399, 406
 Post-test 513
 Power supply 469, 472
 Power users 404
 Pre-installation 399, 402
 pre-installation checklist 401
 Pre-test 513
 Preemptive process management 379
 Premaster secret 340
 Preparedness test 512
 Presentation control 209
 Preventive control 35, 61
 Primary key 217
 Private key 334
 Procedure 129, 166
 Process audit 284
 Process management 378, 385
 Processing 179
 Processing control 201, 236, 566
 Program Code Analysis (PCA) 51
 Promotion 130
 Protection system 385

668 *Index*

Protocol Data Unit (PDU) 255
Proxy server 274
Public key 334
Public Key Infrastructure (PKI) 331,
334, 574, 593
PUT 361

Q

Quality 31
Quality assurance 39, 422, 465, 482,
554
Quality management 16
Quarterly backup 433
Questionnaire 85

R

RADIUS 290
RAID 509, 511
RAM 183, 270
Range check 192
RBI 101, 105, 110
RDBMS 584
Re-engineering 117, 138, 215
Real-time (RT) Systems 376
Reasonableness 194
Reasonableness check 243
Reciprocal arrangements 502
Record count 202, 204
Record retention policy 238
Recovery Point Objective (RPO)
495, 504
Recovery strategies 498, 500
Recovery Time Objective (RTO) 495
Recruitment 130
Red-team penetration testing 347
Redundancy 283
Redundancy check 212
Reference checks 573
Referential integrity 217, 570, 571
Regulatory capital 475
Relational integrity 217

Reliability 32
Remote Procedure Calls (RPC) 255
Repudiation 115, 333
Reputation risks 476
Request For Proposal (RFP) 143,
144, 162, 551
Resolution time 457, 458
Response time 457, 458
Responsibility 71, 73
Restricted groups 414
Restriction control 208, 237
Retention date 196
Reusability 449, 450
Review audit 556
RFC 1918 277
Ring topology 251
Risk 82, 83, 86, 97, 124, 139
Risk assessment 81, 116
Risk management 2, 3
ROI 119, 344
Round Robin 379
Router 255, 260, 266, 276, 282,
368, 422
Router tables 282
RPMs 393
RSA 334
Run to run totals 201
Runtime interpreters 314
RYGB 199, 235

S

SAC 58
Safeguards 82
SAMBA 388
Sample 45
Sample standard deviation 47
Sampling 44, 45, 48, 79
SAN 515
Sandbox 177, 178
Sanitization 453
SANS 349

- SAS 145
- SAS 55 57, 58
- SAS 78 57, 58
- Scheduling 422, 439
- Scorecard approach 476
- SDLC 89, 592
- Secure Sockets Layer (SSL) 338, 593
- Security 31
- Security administrators 344
- Security logs 206
- Security policy 102, 105, 106, 545–547
- Security Test and Evaluation (ST and E) 90
- Segregation 438
- SEICMM 554
- Semi-synchronous replication 517
- Sequence check 192, 194, 243
- Sequential file 434
- Server 422
- Server room 476
- Session hijacks 593
- Set mapping 192
- Setuid 408
- SHA 334, 336
- Shielded twisted pair 257
- Short-range planning 117, 545
- Sign check 243
- Sign-on 191
- Signature-based IDS 278
- Simple transactional websites 318
- Single-user application 173
- Size check 243
- Size cheque 193
- Size of record 194
- Skipping 199
- SLA 144, 288, 289, 290, 457, 458, 462, 482, 488, 501, 583, 585
- Smart Card 182
- Smoke alarms 477
- Smoke detectors 469
- SMTP 49, 315, 362, 363, 588, 589
- Snapshot 219
- Sniffers 396
- SNMP 276, 415
- SNMP community strings 368
- Social engineering 87, 269
- Software 422, 425, 426, 442, 455
- Software firewall 273
- Software metering 446
- Specialized Audit Software (SAS) 52
- Spoofing 87
- Spool files 211
- Sprinkler system 468
- SPX 255
- Spy software 396, 397
- SRS 555
- SSH 365
- SSL session 340
- Stakeholders 115
- Standard 166
- Standardized approach 475
- Star topology 252
- State 275
- Stateful inspection 274
- Stateful inspection firewall 276
- Static web page 309
- Statistical sampling 47
- Stop-or-go sampling 48
- Storage 448, 449, 451
- Storage media 483
- Storage over Internet protocol 518
- Store and forward switch 259
- Strategic plan 127
- Strategy 39, 78, 169, 459
- Stress limit 212
- Subnet mask 266
- Substantive test 43, 216, 219, 228, 441
- Sudo 408
- SUID 357
- SUN iPlanet 358
- Super user 405

670 *Index*

- Switch 255, 282
 - Switched ethernet 367
 - Symmetric encryption 336
 - Synchronous optical network (Sonet) 518
 - Synchronous replication 496, 516
 - System 389
 - System administration 425, 562, 590
 - System administration manual 442
 - System administrators 343
 - System analyst 167
 - System auditing 401
 - System intrusion 87
 - System log 206
 - System penetration 87
 - System services 401, 415
 - System vulnerabilities 284
 - Systems Control Audit Review File Approach (SCARF) 222
- T**
- Tabbing 199
 - TACACS 290
 - Tagging and tracing 219, 222
 - TBA 25, 148, 199
 - TBA applications 23
 - TCP 255
 - TCP wrappers 363
 - TCP/IP 174, 303, 364, 384
 - TCP/IP protocol 264
 - TeamMate 55
 - Technology 31
 - Telnet 88, 255, 315, 362, 415
 - Temporal restriction 186
 - Terminal restriction 186
 - Test 513
 - Test data 51, 219
 - Testing and maintenance 512
 - TFTP 276
 - TFTP server 368
 - The Information System Audit and Control Association 18
- Thin clients 175
 - Threat 85, 87, 93, 96
 - Threat-source 86
 - Threats 82
 - Token 251
 - Top-down 128
 - Topology 84, 248, 249, 253, 283
 - Total Branch Automation (TBA) 22, 174, 224
 - Trailer label 202
 - Training 135
 - Trojan Horse 268
 - TSP 320, 324, 328
 - Turn around time 457, 458
 - Turnover process 464
 - Twisted pair cable 257
- U**
- UDP 275, 362, 588
 - Unicast mode 259
 - UNIX 176, 357, 358, 364, 378, 379, 384, 385, 388, 389, 391, 393
 - Unnecessary services 284
 - Unshielded twisted pair 257
 - Unstratified mean per unit 49
 - UPS 427, 470, 477, 478, 559
 - URL 308, 314, 315
 - Usage control 186
 - USB ports 384
 - User Acceptance Testing (UAT) 593
 - User IDs 426
 - User Interface (UI) 390
 - User rights 411
 - Utility software 395
 - UUCP 364
- V**
- Valid signs—numeric 194
 - Validation 191, 225
 - Validity check 243

Variable sampling 48
Version check 243
Version control 580, 581
VFAT 390
Viability 449, 450
Video surveillance 559
Virtual Router Redundancy Protocols (VRRP) 526
Virus 270
VLANs 259, 320, 342
Voice mail 576
VSNL (Videsh Sanchar Nigam Limited) 311
Vulnerability 82, 85, 86, 88, 89, 90, 93, 96, 284, 345
Vulnerability scanning 346
Vulnerability testing 347

W

WAN 246, 252, 282, 320, 322, 323, 324, 325, 327, 328, 392, 518, 546

Warm site 504, 537
Web browser 330
Web host 308, 340
Web server 308, 331, 525, 587
Web technology 308
Weekly backup 431
Win2k 409
Windows 2000 374, 378, 389, 414, 416
Windows 3.11 389, 392
Windows 95 389
Windows 98 378, 389
Windows NT 358, 378, 389
Windows XP 389
World Wide Web (WWW) 313, 315, 371, 372
WORM 350
Worm 270

X

XTerms 391

