MODULE IV

ISA

INFORMATION SYSTEMS AUDIT 2.0 COURSE

PROTECTION OF INFORMATION ASSETS

BACKGROUND MATERIAL

Committee on Information Technology
The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

Background Material
On
Information Systems Audit 2.0 Course

Module-4 Protection of Information Assets (20%)

The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

Note: There are six other modules which form part of ISA Background Material

DISCLAIMER

The views expressed in this material are those of author(s). The Institute of Chartered Accountants of India (ICAI) may not necessarily subscribe to the views expressed by the author(s).

The information in this material has been contributed by various authors based on their expertise and research. While every effort have been made to keep the information cited in this material error free, the Institute or its officers do not take the responsibility for any typographical or clerical error which may have crept in while compiling the information provided in this material. There are no warranties/claims for ready use of this material as this material is for educational purpose. The information provided in this material are subject to changes in technology, business and regulatory environment. Hence, members are advised to apply this using professional judgement. Please visit CIT portal for the latest updates. All copyrights are acknowledged. Use of specific hardware/software in the material is not an endorsement by ICAI.

Revised Edition	:	July 2015
Committee/Department	:	Committee of Information Technology
E-mail	:	cit@icai.org
Website	:	www.icai.org/http://cit.icai.org
Price	:	₹ 750/- (For Module - I to Module VII, Including DVD)
ISBN	:	978-81-8441-335-9
Published by	:	The Publication Department on behalf of the Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi-110 002.
Printed by	:	Finesse Graphics & Prints Pvt. Ltd. Tel.: 022-4036 4600 Fax : 022-2496 2297

Foreword

Information technology (IT) plays a vital role in supporting the activities of any organisation. The growth and change that has come about as a result of developments in technology have important implications. At the same time the increasing use of IT has also led to e-crimes like cyber warfare, hacking, data thefts, DDoS (Distributed Denial of Service) and other computer related frauds. Subsequently, there are various e-Governance, regulatory and compliance issues which are required to be looked into. These technological changes have put more focus on the role performed by Chartered Accountants, especially in the field of Information Systems Audit.

For Chartered Accountants there exist opportunities in Auditing and Assurance as well as consulting areas. Chartered Accountants with their expertise in data and indepth understanding of systems and process functions are uniquely suited for providing consulting in control implementation of IT enabled services as well as review of the same. IT by default rather than by design has become critically relevant for CA firms.

The Committee on Information Technology (CIT) of the Institute of Chartered Accountants of India (ICAI) was established to identify the emerging professional opportunities in the IT sector. It has also been conducting post qualification course on Information Systems Audit thus providing vast opportunities to Chartered Accountants. In view of the dynamism of the sector, a revised edition of the background material for the post qualification course on Information Systems Audit is being brought up by the CIT.

The background material contains various practical aspects, new technologies along with case studies related to Information Systems Audit, which will make this a great learning guide. I appreciate the efforts put in by CA. Rajkumar S. Adukia, Chairman, CA. Atul Kumar Gupta, Vice Chairman, other members and officials of CIT and faculty for bringing out the revised background material.

I hope that it will be a useful learning material and will assist the members in understanding the nuances of the Information Systems Audit. I wish our members great success in the field of Information Systems Audit.

Best Wishes

CA. Manoj Fadnis
President, ICAI

Preface

Information Technology has now emerged as the Business Driver of choice by Enterprises and Government Departments to better manage their operations and offer value added services to their clients/citizens. We now find increasing deployment of IT by enterprises and governments alike in geometric progression.

While the increasing deployment of IT has given immense benefits to enterprises and government departments, there have been increasing concerns on the efficiency and effectiveness of the massive investments made in IT, apart from the safety and security of Information Systems themselves and data integrity. As enterprises are increasingly getting dependent on IT Resources to manage their core business functionality, there are also concerns of Business Continuity.

It is a matter of immense pleasure for me that the Committee on Information Technology of the Institute has come out with the updated ISA Course 2.0 to equip members with unique body of knowledge and skill sets so that they become Information Systems Auditors (ISAs) who are technologically adept and are able to utilise and leverage technology to become more effective in their work and learn new ways that will add value to clients, customers and employers. This will also meet the increasing need of CAs with solid IT skills that can provide IT enabled services through consulting/assurance in the areas of designing, integrating and implementing IT Solutions to meet enterprise requirements.

The updated course material has taken into consideration the latest curriculum of similar professional courses and the recent/emerging developments in the field of Information Technology and IS Auditing and has been updated taking into consideration all the suggested changes and encompasses existing modules, contents and testing methodology.

The specific objectives of the updated ISA course 2.0 is: “To provide relevant practical knowledge and skills for planning and performing various types of assurance or consulting assignments in the areas of Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems and in an Information Technology environment by using relevant standards, frameworks, guidelines and best practices.”

The updated ISA Course 2.0 has a blend of training and includes e-Learning, facilitated e-Learning, hands on training, project work in addition to class room lectures. This background material also includes a DVD which has e-Learning lectures, PPTs and useful checklists. The focus is to ensure that practical aspects are covered in all the modules as relevant. I am sure the updated ISA course 2.0 will be very beneficial to the members and enable them to offer IT assurance and advisory services.

I am sure that this updated background material on Information Systems Audit Course 2.0 would be of immense help to the members by enhancing efficiency not only in providing compliance, consulting and assurance services but also open out new professional avenues in the areas of IT Governance, assurance, security, control and assurance services.

Information Technology is a dynamic area and we have to keep updating our auditing methodologies and skill-sets in tune with emerging technologies. We hope this updated ISA 2.0 course is a step in this direction. We welcome your comments and suggestions.

CA. Rajkumar S. Adukia
Chairman
Committee on Information Technology

Table of Contents

PROTECTION OF INFORMATION ASSETS
SECTION 1: OVERVIEW

CHAPTER 1: INFORMATION RISK MANAGEMENT AND CONTROLS

CHAPTER 2: INFORMATION SECURITY MANAGEMENT

CHAPTER 4: PHYSICAL AND ENVIRONMENTAL CONTROLS

CHAPTER 5: LOGICAL ACCESS CONTROLS

CHAPTER 6: NETWORK SECURITY CONTROLS

SECTION 2 : APPENDIX

INTRODUCTION TO BACKGROUND MATERIAL

Need for DISA 2.0 Course

Enterprises today in the rapidly changing digital world are inundated with new demands, stringent regulations and risk scenarios emerging daily, making it critical to effectively govern and manage information and related technologies. This has resulted in enterprise leaders being under constant pressure to deliver value to enterprise stakeholders by achieving business objectives. This has made it imperative for management to ensure effective use of information using IT. Senior management have to ensure that the investments and expenditure facilitate IT enabled change and provide business value. This can be achieved by ensuring that IT is deployed not only for supporting organisational goals but also to ensure compliance with internally directed and externally imposed regulations. This dynamic changing business environment impacted by IT provides both a challenge and opportunity for chartered accountants to be not only assurance providers but also providers of advisory services.

The updated ISA course 2.0 has been designed for CAs to provide IT enabled services with the required level of confidence so that management can have trust in IT and IT related services. The ISA course 2.0 builds on the existing core competencies of CAs and provides the right type of skills and toolsets in IT so that CAs can start exploring the immense potential of this innovative opportunity. A key component of this knowledge base is the use of globally accepted good practices and frameworks and developing a holistic approach in providing such services. The background material has been designed with practical perspective of using such global best practices.

Need for updation to DISA 2.0 course

The need for DISA course updation has been extensively discussed considering the objectives and utility of the course. It was decided to update the contents based on suggestions received considering the latest developments in the field of IT and IS Auditing. The updated course has revised modules with key areas of learning as practically relevant for CAs which will enable them to be more effective in their practice for regular compliance audits and also enable to provide IT assurance or consulting services. The updated syllabus has also considered the IT knowledge acquired by the latest batch of CA students who have studied IT in IPCC and Final and have also gone through practical IT trainings. A bridge DISA course is expected to be developed to help existing DISAs to update their knowledge and skills as per the latest course.

Objective of updated DISA Course

The objective of the updated DISA course 2.0 is to equip CAs with a unique body of knowledge and skill-sets so that they can become Information Systems Auditors (ISAs) who are technologically adept and are able to utilise and leverage technology to become more effective in their work and learn new ways and thus add value to their clients or employers. The updated DISA 2.0 course will also meet the increasing market need of CAs with solid IT skills who can provide consulting/assurance in the areas of designing, integrating and implementing IT Solutions to meet enterprise requirements. The updated syllabus of the DISA Course 2.0 has been prepared based on inputs from senior faculty and has undergone numerous reviews over a period of more than two years. The latest curriculum of similar professional courses and the recent/emerging developments in the field of IT and IS Auditing were also referred in updating the course.

Objective of updated DISA Course Material

The primary objective of the updated study material for DISA course is to ensure that DISAs are well versed with the latest IT concepts and practice in the areas of Governance of Enterprise IT, GRC, Assurance, risk, security and controls. The study material has a companion DVD which includes all the reading material and supplementary reference materials and checklists in soft copy. The DVD also includes the e-Learning content available as on date. All the contents in the DVD are presented and linked to aid in easy access of required material. Hence, the DVD and background material will be useful not only as a reading material for passing the DISA exam but also as a reference material for providing IT assurance and consulting services. The sample checklists given in the material can be customised based on scope, objectives of the assignment and considering the nature of business and the technology platform or the enterprise architecture.

Reading of this material is not a one-time exercise but has to be repeated and supplemented with other relevant material and research on the internet. As IT is a rapidly changing area, the material will be updated regularly. Although technology and the services provided using technology undergo rapid changes, the key concepts and requirements for risks, security and control will always remain whether it was the main-frame environment earlier or the mobile computing environment now. Hence, the need for audit and IS audit will always remain.

Use of structured approach

The updated syllabus has been developed by using process oriented structured approach based on the bloom taxonomy of learning and other global best practices. This covers the process/ guidelines to be adapted in development of updated study material.

Overall Objectives

The IT knowledge and skills acquired in the DISA course would enable DISAs to be more effective in using IT for auditing in a computerised environment in existing domains of compliance, consulting and assurance services. The overall objective of the DISA course 2.0 is: **“To provide relevant practical knowledge and skills for planning and performing various types of assurance or consulting assignments in the areas of Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems and in an Information Technology environment by using relevant standards, frameworks, guidelines and best practices.”**

Course Coverage

The DISA Course will provide basic understanding of how information technology is used and deployed. It facilitates understanding of how an IS Auditor is expected to analyse, review, evaluate and provide recommendations on identified control weaknesses in different areas of technology deployment. However, it is to be noted that the DISA course is not oriented towards teaching fundamentals of technology. The DISA course is conducted through a good blend of e-learning (online and facilitated), classroom training, hands-on training with practical case studies and project work to ensure practical application of knowledge. The DISA course combines technology, information assurance and information management expertise that enables a DISA to become trusted Information Technology advisor and provider of IS Assurance services. The DISA with the unique blend of knowledge would serve as the "bridge" between business and technology leveraging the CA's strategic and general business skills. The class room training has been supplemented with hands on training. Aspiring DISAs need to remember that the class room training is not expected to be comprehensive but as aid to facilitate understanding. Considering the extensive coverage of the course, duration and the diverse level of participants, the faculty will not be able to cover the material indepth. **Please read the background materials of the specific modules prior to attending the classes to derive maximum benefit from the class room training.**

DISA Certification

DISA Certification through judicious blend of theoretical and practical training provides CAs with better understanding of IT deployment in enterprises which will enable them to be more effective not only in auditing in a computerised environment covering traditional areas of financial/ compliance audits but also in offering IT enabled services. The DISA exam is designed to assess and certify CAs for conducting IS Audit. After successfully completing the course, the DISA candidates are expected to have required knowledge and skills to perform various assurance and consulting assignments relating to Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems, Information Technology and related areas.

DISA Course : Basic competency requirements

After successful completion of the course, the DISA candidates will have conceptual clarity and will demonstrate basic competency in the following key areas:

- Overall understanding of information system and technology: concepts and practice
- Risks of deployment of information system and technology
- Features and functionalities of security and controls of IT components and IT environment.
- Controls which could be implemented using the security features and functionalities so as to mitigate the risks in the relevant IT components and environments.
- Recommend IT risk management strategy as appropriate.
- Apply appropriate strategy, approach, methodology and techniques for auditing technology using relevant IS Audit standards, guidelines and procedures and perform IS Assurance and consulting assignments.

Modules of the DISA Course

The updated ISA certification is granted exclusively to CAs who demonstrate considerable expertise in domain areas of IT Governance, Security, Control and assurance through their knowledge, skills and experience The primary purpose of the ISA exam is to test whether the candidate has the requisite knowledge and skills to apply IS assurance principles and practices in the following modules:

No.	Name of Module	(%) Q's
1	Primer on Information Technology, IS Infrastructure and Emerging Technologies	20
2	Information Systems Assurance Services	13
3	Governance and Management of Enterprise Information Technology, Risk Management and Compliance Reviews	13
4	Protection of Information Systems Infrastructure and Information Assets	20
5	Systems Development: Acquisition, Maintenance and Implementation.	14
6	Business Applications Software Audit	13
7	Business Continuity Management	7

Learning Objectives

The DISA course is not expected to be an in-depth comprehensive coverage of different aspects of IT such as computer hardware, operating system, network, databases, application software, etc. but is focused on training on how to review IT controls and provide assurance on secure technology deployment.

The key learning objectives are:

1. Demonstrate understanding of functioning of key components of existing and emerging information technology and their practical deployment.
2. Provide IS assurance or IT Enabled services and perform effective audits in a computerised environment by using relevant standards, guidelines, frameworks and best practices.
3. Evaluate structures, policies, procedures, practices, accountability mechanisms and performance measures for ensuring Governance and management of Information Technology, risk management and compliance as per internal and external stakeholder requirements.
4. Provide assurance, consulting or compliance services to confirm that enterprise has appropriate security and controls to mitigate risks at different layers of technology as per risk management strategy.
5. Provide assurance or consulting services that the management practices relating to systems development: acquisition, maintenance and implementation are appropriate to meet enterprise strategy and requirements.

6. Provide assurance or consulting services to validate whether required controls have been designed, configured and implemented in the application software as per enterprise and regulatory requirements and provide recommendations for mitigating control weaknesses as required.

7. Provide assurance or consulting services to confirm whether the Business continuity management strategy, processes and practices meet enterprise requirements to ensure timely resumption of IT enabled business operations and minimise the business impact of a disaster.

8. Plan and perform IS assurance or consulting assignments by applying knowledge learnt by presenting project assignment relating to allotted case study to confirm understanding.

Skill Levels

The updated syllabus provides specific skills in each of the three categories of skill areas. The suggested skill levels ensure that the updated syllabus through all the modules has right blend of concepts and practice. The skill levels will be considered by the authors of study material and also in testing methodology through the eligibility tests and assessment test.

Weightage and category of skills

No.	Skills Category	Weightage (%)
1	Knowledge and Understanding	30 to 40
2	Application of the Body of Knowledge	55 to 60
3	Written communication	5 to 10

Summary of revised DISA Training

No.	Mode of Training	Weightage (%)
1	e-Learning Online (self)	12
2	e-Learning facilitated (lectures)	12
3	Classroom Training (lectures)	42
4	Hands-on Training (on laptop)	24
5	Project Work (self in groups)	10
	Total	**100**

Key highlights of DISA training

DISA Training includes e-Learning, hands on Training, project work in addition to classroom lectures.

- Candidates will have to successfully complete e-learning mode before joining classroom training.
- The training in classroom and hands-on training will follow the order in sequential order of the modules. This includes an inter-mix of classroom lectures and hands-on training. The hands-on training pre-supposes and builds on understanding of concepts of the classroom lectures.
- The training includes mandatory e-Learning of 12 hours for Module-1 and 6 hours for Module-2 and passing in the online test is mandatory and part of the eligibility score.
- Module-4 will have class room lectures of 2 days and hands on training of 2 days. Module-6 will have hands on training of 2 days. **Supplementary e-Learning Lectures covering Modules 4 and 6 are also included.** These will be added in due course and will be made available through DVD or online.
- **Hands on training for Module 4 and 6 will be conducted by the experienced faculty at same venue as class rooms with all participants performing exercises on their own laptops with pre-loaded software and sample/test data as specified in advance.**

DISA 2.0 Course Background Material

The DISA Course 2.0 Background Material is intended to assist in preparing for the DISA exam. The material is a one source of preparation for the exam, but should not be considered as the only source nor should it be viewed as a comprehensive collection of all the information that is required to pass the exam. Participants are encouraged to supplement their learning by using and researching the references provided in the material.

DISA 2.0 Course DVD

The Reading material for the DISA 2.0 course includes a DVD which is comprehensive collection of educational material for revised DISA Course 2.0. This DVD will aid self-learning and includes Background Material, Reference Material, e-Lectures, PowerPoint Presentations, Podcasts/MP3 Files and Self-Assessment Quiz (). This DVD is designed to be supplementary to the background material. It has to be used for self-learning and also as a training aide for the DISA Course 2.0 and DISA candidates are strongly advised to use this for studying for the ISA course.

Standard PPTs for each of the modules of the DISA 2.0 course have been prepared by the authors based on the background material. These are provided in the DVD only and are expected to serve as reference material during the class. Additional references materials and checklists of the course are only included in the DVD. The PPTs may be customised or updated by the faculty as required. Participants are encouraged to copy the DVD contents in their laptops and use this as reference in the classroom training.

Feedback and updates

We compliment you on choosing to join the DISA 2.0 Course and wish you a great learning experience. Please make best use of the material and the training. **Please note that the training is expected to supplement your reading of the material prior to attending the course.** Please participate actively in the training to make the best use of the training The material will be useful to you not only to aid you in preparing for exam but also for providing services in the area of Governance, Assurance and consulting.

Please note that the **background material has been contributed by practising professionals who have shared their expertise and reflects different writing styles of the authors.**

Please provide your feedback on areas of improvement of the course and the reading material in the specified format so that further improvements can be made. Please email your feedback or queries to: **isa@icai.in.** Please visit CIT portal http://cit.icai.org/ for the latest updates of the DISA course. We wish you a great learning experience and a rewarding career as an IS Auditor.

Committee of Information Technology, ICAI

The course material includes references to some specific companies, hardware or software. This reference is only for educational purposes and is not in any way endorsement of the company or products. All copyrights are acknowledged and belong to the rightful owners.

Module 4:

Protection of

Information Assets (20%)

Section 1: Overview

SECTION 1: CONTENTS

CHAPTER 1: INFORMATION RISK MANAGEMENT AND CONTROLS

1.1 Introduction

Use of information technology has become way of life and organisations have adapted the business methodologies by adopting changes in technology. Technology is said to be a double-edged sword. It can help organisations to lead or it may lead to organisations to bleed. Hence, it is important to be at the leading edge of IT but avoid being at its bleeding edge. Technology has inherent risks and hence has to be adequately protected with the right level of controls. In order to reap the benefits of technology organisations must establish processes for protecting the interest of stakeholders to avoid the losses to business due to misuse of technology.

We have seen in earlier modules (module 3) the process for risk management covering the identification and assessment of relevant risk due to technology and how these can impact the organisation. Once the risks are assessed they must be responded so as to ensure that possible losses in case of risk materialization are within acceptable limits of risk appetite and risk tolerance.

1.2 Risk Management

There are typically four types of risk responses:

1. **Avoid:** Organisation may consider this response by deciding not to use technology for select business operation.
2. **Transfer:** Where organisation try to pass on the risk to another entity. For example insuring against financial losses with insurance company by paying suitable premium. Another example could be using outsourcing option, however in this organisation transfers technological risk but in turn introduces managerial risks, hence it may be considered as risk sharing.
3. **Accept:** If the risk assessed is within the risk appetite, management may decide not to implement control and accept the risk.
4. **Mitigate:** Where organisation decide to implement controls, sometimes by incurring additional cost (like delay in process, acquiring tool, adding manpower etc.) so as to reduce the assessed impact to bring it within acceptable limits. Organisation may choose to accept remaining risk.

It is possible that organisation may select more than one response to manage a risk, for example organisation may choose to implement control (Mitigate) and also insure against losses/damage (Transfer). Risk mitigation primarily focuses on designing and implementing controls to prevent incidents due to risk materialisation and/or detect when incident happens of likely to happen and define process to recover from incidence. We will understand in this chapter the concepts associated with identification, selection and implementation of controls.

1.3 Introduction to Information Systems Controls

Control is defined as a mechanism that provides reasonable assurance that business objectives will be achieved and undesired events are prevented or detected and corrected. Control includes policies, procedures, practices and enterprise structure and activities that ensure the desired outcome from business process is not affected. Thus an information systems auditing includes reviewing the implemented system or providing consultation and evaluating the reliability of operational effectiveness of controls.

1.3.1 Need for control and audit of Information systems

Technology has impacted what can be done in business in terms information and as a business enabler. It has increased the ability to capture, store, analyse and process tremendous amounts of data and information by empowering the business decision maker. With the advent of affordable hardware, technology has become a critical component of business. Today's dynamic global enterprises need information integrity, reliability and validity for timely flow of accurate information throughout the organisation. Safeguarding assets to maintain data integrity to achieve system effectiveness and efficiency is a significant control process.

The factors influencing an organisation toward control and audit of computers and the impact of the information systems audit function on organisations are depicted in the Figure 1.1 below.

i. **Organisational Costs of Data Loss:** Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.

ii. **Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations and correction of out-of-control processes. These high level decisions require accurate data to make quality decision rules.

iii. **Costs of Computer Abuse:** Unauthorised access to computer systems, computer viruses, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, documentation etc.).

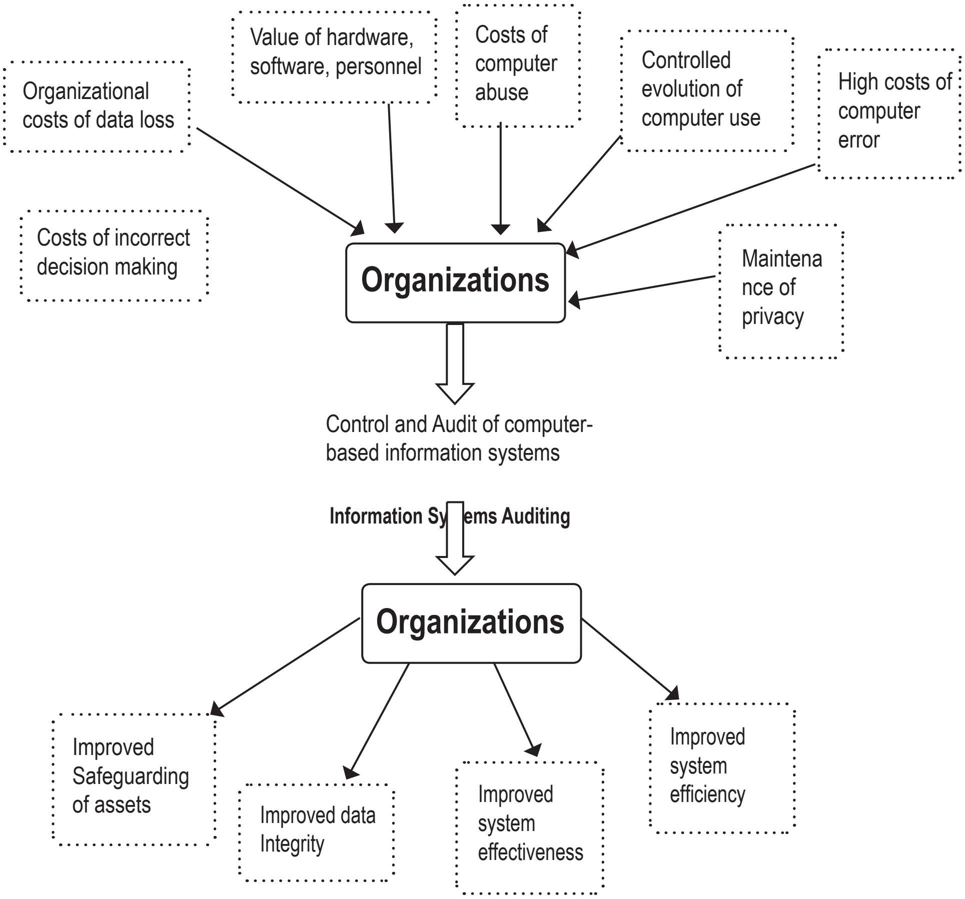

Value of hardware, software, personnel
Costs of computer abuse
Controlled evolution of computer use
High costs of computer error
Organizational costs of data loss
Costs of incorrect decision making
Organizations
Maintena nce of privacy
Control and Audit of computer-based information systems
Information Systems Auditing
Organizations
Improved Safeguarding of assets
Improved data Integrity
Improved system effectiveness
Improved system efficiency

Figure 1.1: Need for control and audit of Information Systems

iv. **Value of Computer Hardware, Software and Personnel:** These are critical resources of an organisation which has a credible impact on its infrastructure and business competitiveness.

v. **High Costs of Computer Error:** In a computerised enterprise environment where many critical business processes are performed a data error during entry or process would cause great damage.

vi. **Maintenance of Privacy:** Today data collected in a business process contains details about an individual on medical, educational, employment, residence etc. These data were also collected before computers but now there is a fear that privacy has eroded beyond acceptable levels.

vii. **Controlled evolution of computer Use:** Technology use and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

viii. **Information Systems auditing:** Is the process of attesting objectives (those of the external auditor) that focus on asset safeguarding and data integrity, and management objectives (those of the internal auditor) that include not only attest objectives but also effectiveness and efficiency objectives.

ix. **Asset Safeguarding Objectives:** The information system assets (hardware, software, data files etc.) must be protected by a system of internal controls from unauthorised access.

x. **Data Integrity Objectives:** Is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organisation depends on the value of information, the extent of access to the information and the value of data to the business from the perspective of the decision maker, competition and the market environment.

xi. **System Effectiveness Objectives:** Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet substantial user requirements.

xii. **System Efficiency Objectives:** To optimise the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.

1.3.2 Objectives of Control

Control objective is defined as "A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT process or activity". Control objectives describe what is sought to be accomplished by implementing the control and the purpose thereof. It serves two main purposes:

(i) Outline the policies of the organisation as laid down by the management.

(ii) A benchmark for evaluating whether control objectives are met.

The objective of controls is to reduce or if possible eradicate the causes of the exposure to probable loss. All exposures have causes and are potential losses due to threats materialising. Some categories of exposures are:

- Errors or omissions in data, procedure, processing, judgment and comparison.
- Improper authorisations and improper accountability with regards to procedures, processing, judgment and comparison.
- Inefficient activity in procedures, processing and comparison.

Some of the critical control considerations in a computerised environment are:

- Lack of management understanding of IS risks and lack of necessary IS and related controls.
- Absence or inadequate IS control framework.
- Absence of or weak general and IS controls.
- Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff.
- Complexity of implementation of controls in distributed computing environments and extended enterprises.

- Lack of control features or their implementation in a highly technology driven environments.
- Inappropriate technology implementations or inadequate security functionality in technologies implemented.

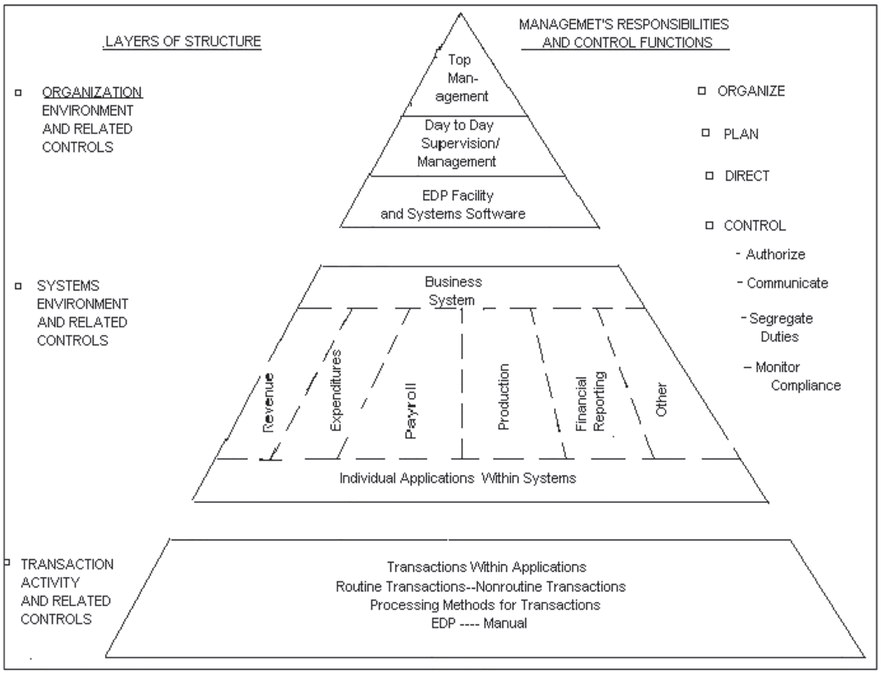

LAYERS OF STRUCTURE
MANAGEMET'S RESPONSIBILITIES AND CONTROL FUNCTIONS
□ ORGANIZATION ENVIRONMENT AND RELATED CONTROLS
Top Man-agement
Day to Day Supervision/ Management
EDP Facility and Systems Software
□ ORGANIZE
□ PLAN
□ DIRECT
□ CONTROL
- Authorize
- Communicate
- Segregate Duties
– Monitor Compliance
□ SYSTEMS ENVIRONMENT AND RELATED CONTROLS
Business System
Revenue
Expenditures
Payroll
Production
Financial Reporting
Other
Individual Applications Within Systems
□ TRANSACTION ACTIVITY AND RELATED CONTROLS
Transactions Within Applications
Routine Transactions--Nonroutine Transactions
Processing Methods for Transactions
EDP ---- Manual

Figure 1.2: Structure of the Control environment

1.3.3 Internal Controls

The basic purpose of an internal control in an organisation 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 organisational structure that gives reasonable assurance to achieve the business objectives. Ultimately, all these policies, procedures etc. are broken into discrete activities and supporting processes, which can be either manual or automated. Control is not solely a policy or a procedure which is performed at a certain point of time; rather it is an ongoing activity, based on the risk assessment of the organisation.

1.3.4 Types of Internal Controls

Controls can be preventive, detective, or corrective (reactive) and have administrative, technical and physical implementations. Examples of administrative implementations are items such as policies and processes. Technical implementations are the tools and software that logically enforce control (such as passwords) and physical implementations include controls such as guard and locked rooms.

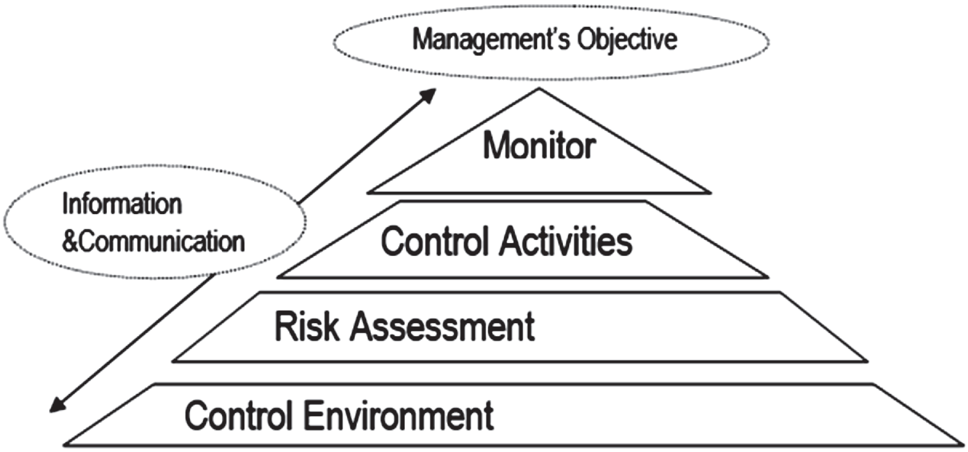


Figure 1.3: Elements of the Internal Control Environment

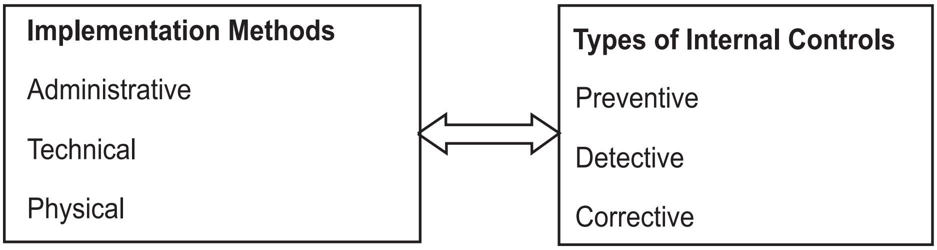


Figure 1.4 : Internal Controls and Implementations

(i) Preventive Controls

These controls are those inputs, which are designed to protect the organisation from unauthorized activities. This attempts to predict the potential problems before they occur and make necessary adjustments. The broad classifications of preventive controls are:

- A clear cut understanding about the vulnerabilities of the asset.
- Understanding possible threats.
- Provision of necessary controls for probable threats from materialising.

Examples of preventive controls include – employing qualified personnel, segregation of duties, access control, documentation etc.

Table 1.1: Preventive Controls

Purpose	Manual Control	Computerised Control
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 authorised person to use the applications	Use access control, viz. User ID, password, smart card, etc.

(ii) Detective Controls

These controls are designed to detect errors, omissions of malicious acts that occur and reporting the occurrence. An example of a detective control would be, audit logs, smoke and fire detectors, or from business perspective use of automatic expenditure profiling where management gets regular reports of spend to date against a profiled spend. The main characteristics of such controls are:

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

Examples of detective controls include: Hash totals, check points in production jobs, error message, duplicate checking of calculations, past-due accounts report etc.

(iii) Corrective Controls

These controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A business continuity plan is considered to be a significant corrective control. The main characteristics of the corrective controls are:

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

Examples of Corrective Controls are-Contingency planning, backup and restoration procedure, rerun procedure, procedure for treating error, etc.

For an auditor to effectively evaluate the efficiency of the objectives of these controls, the following key Table 1.2 might be used keeping in mind the minimum redundancy in the levels of control. The controls rating by an auditor are:

- *High*-Controls implemented over a cause of exposure/error type and should be highly effective.
- *Moderate*-Controls implemented over a cause of exposure/error type and is moderately effective.
- *Low*-Controls implemented over a cause of exposure/error type but have low effectiveness.
- *Blank*-Controls not implemented or does not exist to that cause or exposure or error type.

Table 1.2: Effectiveness and Efficiency of Internal Controls

Methods of Control Implementation	Type of Internal control		
	Preventive	**Detective**	
		With Corresponding Corrective	**Without Corrective**
Manual Control	Blank or Low	Moderate	Blank
	Least effective, generally manual controls applied at front-end of processing; moderately efficient	Moderately effective manual controls; probably least efficient	Least effective and possibly dangerous since users rely on them improperly; very inefficient
Computerized Control	Low or Moderate	High	Blank
	Moderately effective, generally Application controls, applied at front-end of processing; probably most efficient	Most effective, generally controls that are computerised and applied before processing can take place; moderately efficient	May have some effectiveness but probably little; highly inefficient

1.4 Risk and control ownership

Each risk needs to have an owner who can take a decision on risk response. Generally owner is a person or position within the organisation that has close interest about the processes affected due to risk. The person responsible needs to ensure that the risk response is translated into actual day-to-day actions that will prevent and/or detect the risk. It will be this person's responsibility to ensure and manage the effectiveness of an insurance programme, an outsourced arrangement, a policy statement, exception reporting, assignment of authorities, etc.

1.5 Periodic Review and monitoring of risk and controls

After implementation of the risk responses and management techniques, the managers need to monitor the actual activities to ensure that the identified risk stays within an acceptable threshold. To ensure that risks are reviewed and updated organisations must have a process that will ensure the review of risks. The best processes are:

1. Periodic review: the risk assessment exercise may be conducted after predefined period say annual.
2. All incidents and lesson learned must be used to review the identified risk
3. Change management processes proactively review the possible risks and ensure they are part of organisation's risk register.
4. New initiatives and projects must be considered only after risk assessment.

1.5.1 Controls assessment

The first step in control’s assessment is to review the control catalogue (which is a collective record of all controls implemented) and ensure that associated risk is mitigated either by reducing likelihood or reducing impact or both. Based on this the auditor shall be able to prioritise the controls to be tested. The next step is to review control procedure documents the organisation's control processes with the aim of identifying suitable ways of measuring or testing each control.

1.5.2 Control self-assessment

In case organisation has implemented control self-assessment, the actual testing of the controls is performed by staff whose day-to-day role is within the area of the organisation that is being examined as they have the greatest knowledge of how the processes operate. The two common techniques for performing the evaluations are:

- Workshops, that may be but do not have to be independently facilitated, involving some or all staff from the business unit being tested;
- Surveys or questionnaires completed independently by the staff.

On completion of the assessment each control may be rated based on the responses received to determine the probability of its failure and the impact if a failure occurred. It is critical to note that both these methods can be used for risk identification, risk assessment and control design.

1.6 Role of IS Auditor in Information Risk Management

The role of auditor with regard to Information Risk Management can be:

1. Facilitator for conducting risk assessment workshops as risk professional and also guide the process owner of designing of controls.
2. As Auditor, to provide objective assurance to the board on the effectiveness of an organisation’s Risk Management framework to help ensure that key business risks are being managed appropriately and the system of internal controls is operating effectively.
3. As internal auditor, plan the audit cycle according to the perceived risk, i.e. plan for higher frequency for high-risk area business processes.

Key roles that an auditor can perform are:

1) To give assurance on risk management process
2) To give assurance that the risks are being evaluated correctly
3) Evaluate risk management process
4) Review the management of key risks

There are some roles which an auditor should not perform, to maintain his independence:

1) Setting the risk appetite
2) Imposing risk management process
3) Taking decision on risk responses
4) To implement risk response on management’s behalf

1.7 Summary

Information Security is a paramount risk management concern. Information Risk Management follows information as it is created, distributed, stored, copied, transformed and interacted with throughout its lifecycle. It includes understanding what information is critical to key business initiatives, such as growth through acquisitions or expanding partnerships, where it exists across the organisation, where the points of vulnerability are, and what events could put the business at risk. Investments are prioritised based on the amount of risk a given activity entails relative to the potential business reward, and in keeping with the organisation's appetite for risk. Once enterprise information has been located and a risk assessment performed, next step is to implement controls — including policies, technologies, and tools — to mitigate that risk.

1.8 Questions

1. Which of the following shall BEST help in deciding upon the protection level for information asset?

   A. Location of asset

   B. Impact of risk

   C. Vulnerabilities in asset

   D. Inventory of threats

2. Which of the following is a risk response option?

   A. Determine likelihood of threat

   B. Determine probability of risk

   C. Deciding amount of insurance cover

   D. Prepare risk profile report

3. After a Tsunami, a business decides to shift the location of data centre from coastal area to mid land? Which type of risk response option it has exercised?

   A. Accept

   B. Avoid

   C. Mitigate

   D. Transfer

4. Organisations capacity to sustain loss due to uncertainty and expressed in monetary terms is best known as:

   A. Risk appetite

   B. Risk tolerance

   C. Risk acceptance

   D. Risk mitigation

5. Main use of maintaining and updating risk register is to:

   A. Define controls

   B. Identify risk owner

   C. Built risk profile

   D. Maintain evidence

6. Of the following who is accountable for deciding and implementing controls based on risk mitigation plan?

   A. Chief risk officer

   B. Risk owner

   C. IT operations manager

   D. Board of directors

7. Which of the following is a risk factor that may have impact on organisation?

   A. Management decides to acquire new application software

   B. A new application required by organisation is released

   C. Vendor decides to stop supporting existing application

   D. Organisation retires old application that is not in use

8. While auditing risk monitoring process which of the following IS auditor should review FIRST?

   A. Risk assessment process

   B. Risk management framework

   C. Alignment with business risks

   D. Annual review of risk register

9. The quantum of risk after enterprise has implemented controls based on risk mitigation plan is:

   A. Accepted risk

   B. Residual risk

   C. Inherent risk

   D. Current risk

10. Which of the following shall best help in aligning IT risk with enterprise risk?

    A. Presenting IT risk results in business terms

    B. Conducting business impact analysis

    C. Making chief risk officer accountable

    D. Align IT strategy with business strategy

1.9 Answers and Explanations

1. B. Other options i.e. location of asset, existing vulnerabilities in asset shall be covered during risk assessments. Inventory of threats only will not help, impact due to threat must be assessed.

2. C. Of the four main risk response options accept, avoid, mitigate and transfer, Insurance cover is a risk response option of risk transfer

3. B. BY shifting location the business has avoided the risk associated with Tsunami.

4. A. It is the definition of risk appetite. Risk tolerance is capacity to tolerate down time due to risk materialisation. Risk acceptance and risk mitigation are risk response decision based on risk appetite.

5. C. Main use of risk register is to develop risk profile of the organisation for management's review and enable risk informed decisions.

6. B: Risk owner is primarily accountable for deciding and implementing on nature of controls. Generally risk owner is process owner. Chief risk office guides risk owner, IT head is responsible for responding to risk owned by IT head. Although board of directors is ultimately accountable, for specific risk, risk owners are responsible.

7. C. Vendor decides to stop supporting existing software changes the market situation that will affect organisation, since it has to take decision on replacing application. Release of new application though changes market, it may not affect the organisation immediately as the organisation may not need to take action. Options A and D are internal decisions and will be done after risk assessment and hence these are not risk factors.

8. D. Risk monitoring refers to review of identified and assed risks based on changes, incidents, and periodically. Other options are part of risk management framework.

9. B. Accepted risk is where controls are not implemented is part of residual risk, Inherent risk is total risk before implementing controls. Current risk is residual risk at a point in time during control implementation.

10. A. Expressing IT risk in business terms i.e. as impact on business will help business in understating relevance of IT risks. Business impact analysis may be useful however it may or may not help depending upon scope of project. Making chief risk officer accountable may help but best is A. Aligning IT strategy with business strategy shall help in defining better IT plan, but it is at higher level.

CHAPTER 2: INFORMATION SECURITY MANAGEMENT

2.1 Introduction

Protection of information assets includes the key components that ensure confidentiality, integrity and availability (CIA) of information assets. There are three key objectives of Information Security Management viz.: ***Confidentiality, Integrity and Availability*** also called ***CIA Triad.***

- **Confidentiality:** No data or information is made available to any person within or outside the organisation, other than the persons who are authorised to use that data.
- **Integrity:** No data/information or programme shall be allowed to be modified by anyone without proper authority.
- **Availability:** All Information Systems including hardware, communication networks, software applications and the data they hold, is available to authorised users to carry out business activities.

Controls to protect the assets are designed, developed, selected and implemented based on risk evaluation and cost-benefit analysis. The primary control for implementing protection strategy is defining and implementing information security policy. Organisation need to focus on ensuring that information security practices are followed to meet the security objectives of organisation derived from the stakeholder's expectations. This requires implementing processes for information security management. The key elements of information security management include:

- Senior management commitment and support
- Policies and procedures
- Organisation structure and roles and responsibilities
- Security awareness and education
- Monitoring
- Compliance
- Incident handling and response

2.2 Senior management commitment and support

Commitment and support from senior management are important for successful establishment and continuance of an information security management programme. The tone at the top must be conducive to effective information protection and security management. It is unreasonable to expect lower-level personnel to abide by security measures if they are not exercised by senior management. Executive management endorsement of intrinsic security requirements provides the basis for ensuring that security expectations are met at all levels of the enterprise. Penalties for non-compliance must be defined, communicated and enforced from the board level down. The senior management's support for security initiatives is evident from activities and decisions. Some of the key indicators are:

1. Providing support for defining organisation structure that supports implementation of information security initiatives by establishing Information Security Organization (ISO) and steering committee and assigning responsibility for security operations
2. Regularly reviewing security projects, reports and activities as part of agenda item on board meetings
3. Approving risk response decisions and security policies
4. Practicing security practices
5. Ensuring adequate budget
6. Review of audit reports

2.3 Critical Success Factors to Information Security Management

Information Security can be a business enabler if following five suggested actions are adopted by Information Security Management:

a) **Alignment with business objectives:** Management views Information Security as another support function and not primary business function although an important function. The Management need to establish security policy in line with business objectives, to ensure that all Information Security elements are strategically aligned.

b) **Organisational culture:** Ensure that the framework followed to implement, maintain, monitor and improve Information Security is consistent with the organisational culture.

c) **Establish and enforce an Information Security Programme:** Information Security program focuses on protecting information present in business processes. Establish a program to improve Information Security management enterprise-wide and enforce it.

d) **Adoption of standard:** Adopting an internationally recognised reference framework to establish an Information Security framework is useful in providing assurance that all required aspects of information security are covered. It also helps in benchmarking the security levels. Adopting an information security standard seems to demonstrate to staff, customers and trading partners that their data is safe, and that there is an independent verification of this fact. Rules formulated under IT (Amendment) act, 2008 defines reasonable security as implementation of ISO 27001 or equivalent certifiable standard so as to establish that reasonable security practices are being followed.

e) **Spend resources wisely and transparently:** Prioritise expenditures to mitigate risks and avoid spending more resources in assessing risks than those that would be spent if the problems really occurred.

2.4 IT Security policies, procedures, standards and guidelines

Information Security policy will define management's intent on how the security objectives must be achieved. It will also encompass the view on risk and will define a security framework to meet business objectives. Security policies, guidelines and procedures affect the entire organisation and, as such, should have the support and suggestions of end users, executive management, auditors, security administration, IS personnel and legal counsel. After policies are outlined, standards are defined to set the mandatory rules that will be used to implement the policies. Some policies can have multiple guidelines, which are recommendations as to how the policies can be implemented. Finally, information security management, administrators, and engineers create procedures from the standards and guidelines that follow the policies.

A security policy is a document that defines the scope of security needed by the organisation and discusses the information assets that need protection and the extent to which protection is required. The Information Security Policy is an overview or generalisation of an organisation's security needs. It should clearly define why security is important and what assets are valuable. The formulations of policies are based on outcome of risk management process. Organisations can have polices depending upon culture of organisation, nature of business, compliance requirements, geographical and regional environment within which organisation is operating.

2.4.1 What should the policy contain?

The policy should have a number of different statements covering each of the major aspects of information security. Each policy statement should be derived from a major business objective, as this is the fundamental justification for any security requirement. The relationship between objectives (sometimes called Business Principles), policies, the resulting standards and procedures is best illustrated by an example below.

Example of Business Objective Policy: To be recognised as a good employer staff safety and security come before the security of company assets.

Every organisation may have different polices depending upon nature and focus of business and result of risk management process, however some of the common policies are discussed here.

Data classification and Privacy Policies

It is the policy of the Organisation to protect against the unauthorised access, use, corruption, disclosure, and distribution of non-public personal information in its possession, and to comply with all applicable laws and regulations regarding such information. It generally covers:

- ➢ The organisation shall hold non-public personal information in strict confidence and shall not release or disclose such information to any person except as required or authorized by law and only to such persons who are authorised to receive it.
- ➢ The organisation shall adopt procedures for the administrative, technical and physical safeguarding of all non-public personal information.
- ➢ The organisation shall ensure that an entity controlled by it, or any other entity that utilises information provided by the organisation to carry out its responsibilities, shall have signed and agreed to abide by the terms of the data privacy and security policy or shall have adopted a data privacy and security policy that is substantially similar to the organisation policy.

Acceptable use of information assets policy

An acceptable use policy (AUP), also known as an Acceptable Usage Policy or Fair Use Policy, is a set of rules applied by the owner or manager of a network, website or large computer system that restrict the ways in which the network, website or system may be used. AUP documents are written for corporations, businesses, universities, schools, internet service providers, and website owners, often to reduce the potential for legal action that may be taken by a user, and often with little prospect of enforcement.

Acceptable use policies are an integral part of the framework of information security policies; it is often common practice to ask new members of an organisation to sign an AUP before they are given access to its information systems. For this reason, an AUP must be concise and clear, while at the same time covering the most important points about what users are, and are not, allowed to do with the IT systems of an organisation. It should specifically cover Acceptable Use of Internet. For example it may state that no user of company's Internet facility will connect to pornographic, child abuse, or racial discrimination sites and so on.

Physical access and Security Policy

Physical security describes security measures that are designed to restrict unauthorised access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). Physical security involves the use of multiple layers of interdependent systems which include CCTV surveillance, security guards, Biometric access, RFID cards, access cards protective barriers, locks, access control protocols, and many other techniques.

Asset Management Policy

This policy defines the requirements for Information Asset's protection. It includes assets like servers, desktops, handhelds, software, network devices etc. Besides, it covers all assets used by an organisation-owned or leased.

Business Continuity Management Policy

This policy defines the requirements to ensure continuity of business critical operations. It is designed to minimise the impact of an unforeseen event (or disaster) and to facilitate return of business to normal levels.

Network Security Policy

A network security policy defines the overall rules for organisation's network access, determines how policies are enforced and lays down some of the basic architecture of the company security/ network security environment.

Password Policy

This policy defines high-level configuration of password to be used within organisation to access the information assets. For example:

- Password length must be more than 8 characters
- Password must be complex containing upper case, lower case, numeric and special characters
- Password must be changed regularly

- Password should not be used again for minimum period
- Password should not be changed in consecutive sequence

2.4.2 Controls over Policy

Information security policies need to be maintained and updated regularly. This is required due to changes in environment, IT technology, threat scenarios, business processes, business strategy, and organisational structures. This might need to revisit the security requirements and hence policies. Hence, it is necessary to review the security policies periodically to ensure that they are in line with the management's intent. Typically security policies are reviewed:

- Periodically, generally annually
- After incident
- As a part of change management process

Exceptions

Policies are generic and sometimes cannot be enforced in specific situations, a process for defining and approving exceptions must be defined. In such situations it is necessary to ensure there are suitable compensating controls so that the risks mitigated by enforcement of policy are within acceptable limits. Such exceptions are for predefined period and must be removed over the period of time or reviewed periodically. For example: legacy application does not provide for implementing password policy. An exception may be approved with additional strong compensating control over access granting process or application accesses. This exception may be approved for a specific period of time, during which application may be changed to be compliant with password policy.

2.5 Tools to Implement Policy: Standards Guidelines and Procedures

The next level down from policies is three elements of policy implementation as given here:

Standards: Specify the uniform way for the use of specific technologies in an organisation. This standardization of operating procedures can be a benefit to an organisation by specifying the uniform methodologies to be used for the security controls. Standards are usually compulsory and are uniformity implemented throughout organisation.

Guidelines: Guidelines are similar to standards; they refer to the methodologies of securing systems, but they are only recommended actions and are not compulsory. Guidelines are more flexible than standards.

Procedures: Procedure contains the detailed steps that are followed to perform a specific task. Procedures are the detailed actions that must be followed. They are considered the lowest level in the policy chain. Their purpose is to provide detailed steps for implementing the policies, standards, and guidelines previously created.

2.6 Information Security Organisation

Information security is responsibility of entire organisation and accountability of senior management and board of director. Information security officer is facilitator in implementing security across organisation. The Information Security Organisation (ISO) plays a critical role in ensuring an organisation's information and its information assets are properly protected, managing vulnerabilities within the infrastructure, managing threats and incidents impacting resources, ensuring policies are in place and employees comply with them, and educating employees about their information security and privacy protection responsibilities.

The position must be strategically placed within the organisation and visibly supported by top management while carrying out the duties in an effective and independent manner. Possessing both a broad range of business management and technical security skills, and a clear understanding of the organisation's business is critical to an ISO's success.

There is no easy solution to implementing an effective information security program within an organisation. An effective programme cannot be established overnight and will be a continuous ongoing function once established. Appointing a skilled ISO who has the full support of executive management is the first important step necessary to implementing the programme. To ensure that information security is implemented across organisation ISO requires creation of the information security organisation. This can be best done by defining security responsibilities for every person and position as part of his/her role within organisation and documented in their job description. While defining roles and responsibilities following aspects must be considered.

2.6.1 Clearly defined duties

The first fundamental security rule is that each individual should be aware of what the organisation expects from them. These expectations are communicated through various important documents such as company policies and individual job descriptions duties, responsibilities and the level of authority they have. It is difficult (and unjust) for an organisation to accuse an individual of carrying out activities or tasks which they have no right to do, if the individual's job was not clearly possible for an organisation to put into place other personnel security procedures including the following:

- Segregation of duties
- Four eyes (the two person principle)
- Rotation of duties
- Key man policies

Segregation of Duties

No individual, of whatever seniority in the organisation, should have the ability to carry out every step of a sensitive business transaction. For example, a salesman should not be able to enter a customer's order in the order book and have access to the stock control/delivery system and settlement part of the sales ledger. Access to too many functions enables staff to carry out a fraudulent transaction and hide their tracks.

- A programmer should not be allowed to operate a computer system, or to gain access to production systems or data. Similarly, operators, should but act as programmers although, in practice, this rule is becoming undermined by the use of personal computers and small office systems. It is also a difficult rule to apply to an on-line computing environment.

- System security features should be introduced by staff completely independent of programming or operations.
- Devolution of authority from an owner to a custodian of any classified or sensitive material should be include the ability to authorise its reproduction, issue or destruction. Independent checks of this person's work must be carried out at random times.

The 'Four Eyes' (Two-person) Principle

To reduce the opportunities for any person to breach security, those responsibilities and duties which would afford particularly powerful access to the system, or which act at key control points, should not be carried out by one person alone. Examples of this include: two signatories required for a cheque, and two people always being present in a critical computer room.

It must be noticed that there is a possibility of collusion between the staff members. To avoid this, steps should be taken to vary shift rotas and working practices so that the same people are not always working together. Vital functions should also be well dispersed amongst staff members. Although this can be seen as a mistrust of staff it can also provide a protection, as individual with the ability to act alone may be in danger of coercion.

The Rotation of Duties

No one person should be kept in one particular post for too long, especially if that appointment involves any particular security responsibilities opportunities for dishonesty. Job rotation can also help avoid the errors which occur from boredom and over familiarity, and place a limit on any fraudulent activities. The replacement of an individual may well reveal any dishonesty or inefficiency which has been continuing over a period of time.

A similar rule should insist that staff take at least two consecutive weeks; holiday in any year, as experience has shown that many frauds need continual masking by the perpetrator and may surface when the individual is away.

'Key Man' Policies

Organizations should avoid situations where an individual becomes indispensable to the business. A 'key man' policy identifies areas of operational activities where such situation may occur and seeks, where possible to enable cover by other individuals to be established. In cases where it is unavoidable that a single individual is pivotal, insurance policies may be taken out to cover losses resulting from his or her death or incapacity. Key man policies also cover issues such as the protection of groups of key staff such as senior managers and lays down rules under which they will not travel in the same vehicle (aircraft and cars) to limit the impact on the organisation, should there be an accident.

2.6.2 The Concept of Responsibility in Security

Responsibilities are the defined duties of individual within an organisation, once a responsibility is assigned it is usual for an individual to be held to be accountable for satisfactory performance. The main types of role for individuals within a security structure are described below.

Ownership

Organization has acquired a number of assets required for business operations. The organisation is legal owner of these assets. However for security and control the ownership is delegated to an employee or group of employees who need to use these assets. In other words, users have right to not only use the assets but are also responsible for the safe-keeping of assets.

This fundamental rule of organisational control also applies to corporate security, where ownership must be defined in order for control to be applied. Thus every corporate asset, building, item of equipment, bank account and item of information should have a clearly defined 'owner'. The owner should then have a defined set of responsibilities.

- Ensuring that computer rooms are kept clean and tidy
- Ensuring that equipment is well maintained and kept operational
- Ensuring that an item of data used by the organisation is accurate and up to date

Owners of a particular asset generally have authority over it, thus an owner may have the authority to update an item of data. Where too much power may be put into the hands of an individual more than one owner may be appointed (although there can be problems where there is unclear authority). Bad management practice will put an individual in a position where they have no real authority to influence something for which they have been given responsibility. Authorization is the essential statement where an owner gives their assent to an activity happening. Authority and ownership are generally synonymous.

Custodianship

In some instances an owner is not able to manage a particular asset on a day-to-day basis, perhaps for logical or technical reasons. In this case responsibility may be passed on by the owner to a custodian. The owner should clearly state the requirements, the responsibilities and associated levels of authority of the custodian and final management responsibility will always reside with the owner. Examples of custodian include a data centre operations functions controlling access to production data, and a computer bureau running an application for a client.

Controlling

In all security systems there are key tasks which can be called control points. It is at these control points that the actual security mechanism has its application. For example, a security administrator acts as a control on who has access to computer resources. They carry out the task of adding and deleting user identifiers from the system or modifying the task of adding available to them, and therefore effectively control the activities of the owner, or other designated authority.

2.7 Role and responsibilities

To have an effective information security program, the roles and responsibilities of all participants must be clearly defined. Besides, segregation of duties plays an important role in the effective application of information classification and related controls. Some of the key roles and responsibilities are explained here.

2.7.1 Steering Committee

To some extent security affects all aspects of an organisation. To be effective, security must be pervasive throughout the enterprise. To ensure that all stakeholders impacted by security considerations are involved, many organisations use a steering committee comprised of senior representatives of affected groups. This facilitates achieving consensus on priorities and trade-offs. It also serves as an effective communications channel and provides an ongoing basis for ensuring the alignment of the security program with business objectives. It can also be instrumental in achieving modification of behaviour toward a culture more conducive to good security. The committee discusses issues related to protecting information assets, and establishes and approves security practices. The committee should be formally established with appropriate terms of reference

2.7.2 Information Owner

Information Owner (also called Data Owners) is responsible for a company information asset. The responsibilities are generally assigned to person/position that owns business process. Primary responsibilities are:

- Assign appropriate information classification and periodically review the classification to ensure it still meets the business requirements.
- Ensure security controls have been implemented in accordance with the information classification.
- Review and ensure currency of the access rights associated with the information assets they own.

2.7.3 Information custodian

Information custodian is assigned the task of implementing the prescribed protection defined by the security procedure and top level/senior management decisions. He is usually an information technology or operations person, and is the system administrator for the Information Owner.

Among other activities, information custodian also performs following activities:

- Ensuring safe keeping of information on behalf of information owner
- Providing access to users that are approved by owners
- Running regular backups and routinely testing from backup data
- Performing data restoration activity from the backups when necessary

2.7.4 System Owner

The system owner is responsible for one or more systems, each of which may process and store data owned by different information owners. Here a system refers to group of assets required for hosting one or more applications that support a business function. E.g. Human resource data management system is owned by the HR department including Hardware, OS, database, Middleware, application and data. A system owner is responsible for:

- Integrating security considerations into application and system purchasing process and decisions.
- Ensuring that adequate security is built or defined once the applications and systems have been acquired and are ready for use in production environment.

- Ensuring that the systems are properly assessed for vulnerabilities and report any to the incident response team and information owner.

2.7.5 Process owner

This person is responsible for the implementation, management and continuous improvement of a process that has been defined to meet a business requirement.

2.7.6 System Administrator

System Administrator is the one with administrative/root level privileges of the operating systems like Windows, Unix etc. This means that they can add and remove permissions and set security configurations. A system administrator is responsible for:

- Creating new system user accounts
- Changing permissions of existing user accounts
- Implementing new security software
- Testing security patches and updates, and
- Resetting user passwords

2.7.7 User manager

User manager is the immediate manager or reporting manager of an employee. They have ultimate responsibility for all user IDs and information assets owned by company employees. In the case of non-employee individuals such as contractors, consultants, etc., user manager is responsible for the activity and for the company assets used by these individuals.

2.7.8 Super User

The person with the highest level of authorisation access, who can make any transaction and master set up activity immediately and sets the conditions for transaction approvals, financial daily limits of each transaction type, and classifies and authorises other users.

2.7.9 Security Manager

Security manager is responsible for defining security strategy and policies for the organisation. The manager also ensures defining roles and responsibilities.

2.8 Human Resources Security

Employees handling personal data in an organisation need to receive appropriate awareness training and regular updates in an effort to safeguard the data entrusted to them. Appropriate roles and responsibilities assigned for each job description need to be defined and documented in alignment with the organisation's security policy.

The management of human resources security and privacy risks is necessary during all phases of employment association with the organisation. Training to enhance awareness is intended to educate individuals to prevent data disclosure, recognise information security problems and incidents, and respond according to the needs of their work role. Safeguards include the following:

- Job descriptions and screening
- User awareness and training
- A disciplinary process, and
- An orderly exit process must exist to equip employees to operate securely and use information appropriately, and ensure that access privileges change when a user's relationship with the organisation changes

The objective of human resources security is to ensure that all employees and 3rd parties (having access to sensitive data) are qualified for and understand their roles and responsibilities of their job duties and that access is removed once employment is terminated. The three areas of Human Resources Security are:

a) **Pre-employment:** It includes defining roles and responsibilities of the job, defining appropriate access to sensitive information for the job, and determining depth of candidate's screening levels-all in accordance with the company's information security policy.

b) **During employment:** Employees and 3rd parties with access to sensitive information in an organisation should receive periodic reminders of their responsibilities and receive ongoing, updated security awareness training to ensure their understanding of current threats and corresponding security practices to mitigate such threats.

c) **Termination or change of employment:** To prevent unauthorised access to sensitive information, access must be revoked immediate upon termination/separation of an employee and 3rd parties with access to such information. This also includes the return of any assets of the organisation that was held by the employee.

2.9 Training and Education

Since the terrorist attacks, corporations and government organisations alike have brought security training, awareness, and education into the spotlight. Once thought of as “just filling a mandatory requirement” or “I have to do this because my boss told me too,” is not the perception now. Various computer crime studies show that the threat from insiders ranges from 60% to 90%. This does not mean that more than 60% of the employees in an organisation are trying to hack into the system; it does mean that employees, whether intentionally or accidentally, may allow some form of harm to the system. This includes having weak passwords, sharing their passwords with others, installing illegal copy of screensaver software or downloading shareware from the Internet. Thus, employees need to be made aware of the information security policies of the company and how to practice good computer security skills.

An integrated security training, awareness, and education programme must be based on a validated training strategy and include a formal course curriculum in addition to other learning interventions designed to deliver the appropriate security information and messages to all levels of employees. To do this, a broad programme that includes training, education, awareness, and outreach must be developed to deliver a multitude of security messages through various means to all employees. Formal, instructor led training, computer or Internet-based training, videos, conferences, forums, and other technology based and traditional delivery methods are all examples of what must be part of the integrated security training, education, and awareness program. Important considerations for security awareness training programme are:

a) **Mandatory Security Awareness:** Ensure that security awareness training is mandatory for all staff (including management).

b) **Training for Third Parties:** Ensure that all third parties with access to an organisation's information receive the same security awareness training, or training to an equivalent level.

c) **Training is required before access is granted:** Security awareness training commences with a formal induction process designed to introduce the organisation's security policies and expectations before access to information or services is granted.

d) **Acknowledge Policy:** Ensure that all employees are required to acknowledge that they have read and understood the organisation's information security/acceptable use policy.

e) **Training at Least Annually:** Ensure that all employees and third parties (having access to company information and information systems) are given security awareness training at least once per year.

2.10 Systems Configuration

Configuration management is the process of tracking and approving changes to a system. It involves identifying, controlling, and auditing all changes made to the system. It can address hardware and software changes, networking changes, or any other change affecting security. Configuration management can also be used to protect a trusted system while it is being designed and developed. The primary security goal of configuration management is to ensure that changes to the system do not unintentionally diminish security. For example, configuration management might prevent an older version of a system from being activated as the production system. Configuration management also makes it possible to accurately roll back to a previous version of a system in case a new system is found to be faulty. Another goal of configuration management is to ensure that system changes are reflected in current documentation to help mitigate the impact that a change might have on the security of other systems, while in either the production or planning stages.

Configuration management is a discipline applying technical and administrative direction to do the following:

- Identify and document the functional and physical characteristics of each configuration setting
- Manage all changes to these characteristics
- Record and report the status of change processing and implementation

Configuration management involves process monitoring, version control, information capture, quality control, bookkeeping, and an organisational framework to support these activities. The configuration being managed is the verification system plus all tools and documentation related to the configuration process.

2.11 Information Security and external parties

In order to bring efficiencies and economies of scale, many organisations resort to outsourcing and are allowing more and more vendors, customers and other 3rd parties to access the information assets of organisation. This trend has its own operational merits but brings significant information security challenges specifically with regard to confidentiality and integrity of the organisation's information. As a result, many organisations these days are asking all 3rd parties, having access to the organisation's information and information systems, to sign a Non-Disclosure Agreement (NDA). A non-disclosure agreement (NDA), also known as a confidentiality agreement (CA), is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to or by third parties. It's a contract through which the parties agree not to disclose information covered by the agreement. An NDA creates a confidential relationship between the parties to protect any type of confidential and proprietary information or trade secrets. As such, an NDA protects non-public business information.

2.12 Issues and challenges of IS Management

An organisation may face various challenges in Information Security Management. Some common challenges are:

1. **Organization's strategic drivers:** The strategic drivers and needs of the organisation may conflict with the actions required to ensure that assets and processes remain productive. Finding the right balance between protecting the organisation's core assets and processes and enabling them to do their job becomes a challenge for security management-and a significant barrier to effectiveness.
2. **Regulatory Requirements:** Another consideration for security management is the organisation's regulatory environment. Just as the organisation must expose itself to its environment to operate, so must it be willing to accept some of the limitations imposed on like organisations that operate in its competitive space. This brings another level of challenges that affects the organisation's ability to be effective at security management.
3. **Information Security as an afterthought:** The problem of information security being considered as an afterthought dates back to the era of checklists. Once a system has been implemented, it was a norm to follow a checklist to address whether any of the security 'holes' remained unplugged. While the information security community has recognised the inadequacy of checklists as a means to address security concerns, the checklist culture has, however, prevailed. Therein resides the problem of information security being considered as an afterthought.
4. **Lack of Integration in System Design and Security Design:** Development duality is a phenomenon where systems and security design are undertaken in parallel rather than in an integrated manner. This largely occurs when systems developers fail to recognize the security requirements at the onset of the development process.

2.13 Computer crimes and exposures

A computer crime, also called *cyber-crime*, is any unlawful activity that is done using a computer. Computer crime is one of the fastest-growing types of illegal activity, both in the India and internationally. While the Internet links people together like never before, it also provides endless opportunity to criminals seeking to exploit the vulnerabilities of others. These types of crime are notoriously hard to solve and sometimes occur without the victim ever knowing anything illegal has taken place. There are several different types of computer crime, many of which overlap. Some of the most commonly reported computer crimes are:

a. **Denial of Service (DoS):** A Denial-of-Service attack (DoS) is an attempt to make a machine or network unavailable to its intended users. This causes legitimate users to not be able to get on the network and may even cause the network to crash.

b. **Network Intrusions:** Network Intrusion refers to unauthorised access to an organisation's internal network.

c. **Software Piracy:** The illegal copying of software.

d. **Spoofing of IP Addresses:** IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system

e. **Eavesdropping:** Eavesdropping is the unauthorised real-time interception of a private communication, such as a phone call, instant message, and video-conference or fax transmission.

f. **Phishing:** Phishing is the act of trying to obtain information like user ID and password for bank accounts, credit card pin etc. using electronic communication means like emails, fake websites etc.

g. **Social Engineering:** It is the act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information. Social engineering is successful because its victims innately want to trust other people and are naturally helpful. The victims of social engineering are tricked into releasing information that they do not realise will be used to attack a computer network. For example, an employee in an enterprise may be tricked into revealing an employee identification number to someone who is pretending to be someone he trusts or representing someone he trusts.

h. **Hacking:** Hacking is the process of exploiting vulnerabilities of a system to gain unauthorized access to system or resources like a website, bank accounts etc.

i. **Dumpster diving:** Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) It is a technique used to retrieve information that could be used to carry out an attack on an organisation. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organisational chart can be used to assist an attacker using social engineering techniques to gain access to the network.

j. **Data-Diddling:** Data stet diddling is the changing of data before or during entry into the computer system. Examples include forging or counterfeiting documents used for data entry and exchanging valid disks and tapes with modified replacements

k. **Targeted attacks:** The new trend in cyber (computer related) crimes is targeted attacks. These are the attacks that are specifically targeted to selected organisation. It is combination of attacks like malware (a virus or programme that is written with specific objective e.g. Stuxnet), social engineering to introduce malware in system, data diddling and scavenging (malware once activated initiated these attacks and sends information outside in small proportions so as not to detect.

l. **Advanced persistent Threat (APT):** This is a type of targeted attack that continues for a sustained period for about a year or more. A malware launched starts sending confidential information masking it and in small proportions so as not to cross monitoring thresholds.

m. **Botnets:** Acronym for robotic network. An underground network established by hackers by sending malware. This malware goes undetected since it is part of targeted attack. Hackers build a virtual network of such compromised computers and uses as and when required to launch attacks.

2.14 Incident handling and response

A computer security incident is an event adversely affecting the processing of computer usage. This includes loss of confidentiality of information, compromise of integrity of information, denial of service, unauthorised access to systems, misuse of systems or information, theft and damage to systems. Other incidents include virus attacks and intrusion by humans within or outside the organisation. It defines requirements for handling information security incidents. Information security incidents include virus, worm, and Trojan horse attack, unauthorised use of company information systems, and Acceptable Use Policy violations. This policy applies to all Employees and Third Parties who have access to company information and information systems.Incident Handling should address:

a. What constitutes an incident
b. How should an incident be reported
c. To who should an incident be reported
d. What action should be taken if an incident occurs
e. Who should handle the response to the incident
f. Are recovery procedures required
g. What type of follow up or review is required
h. Should additional safeguards be implemented

To minimise damage from security incidents and to recover and to learn from such incidents, a formal incident response capability should be established, and it should include the following phases:

- Planning and preparation
- Detection
- Initiation
- Recording
- Evaluation
- Containment
- Eradication
- Escalation

- Response
- Recovery
- Closure
- Reporting
- Post-incident review
- Lessons learned

The organisation and management of an incident response capability should be co-ordinated or centralised with the establishment of key roles and responsibilities. This should include:

- A coordinator who acts as the liaison to business process owners
- A director who oversees the incident response capability
- Managers who manage individual incidents
- Security specialists who detect, investigate, contain and recover from incidents
- Non-security technical specialists who provide assistance based on subject-matter expertise
- Business unit leader liaisons (legal, human resources, public relations, etc.)

Incidents occur because of weaknesses or vulnerabilities that are not addressed properly. A post-incident review phase should determine which vulnerabilities were exploited and why. Analysing the cause of incidents may reveal errors in the risk analysis or point out need for risk review due to unidentified threat, indicating that the residual risks are higher than the calculated values and inappropriate countermeasures have been taken to reduce inherent risks. In establishing this process, employees and contractors are made aware of procedures for reporting the different types of incidents (e.g., security breach, threat, weakness or malfunction) that might have an impact on the security of organisational assets.

2.15 Implementing information security policies

Appropriate implementation of information security policy helps in minimising internal security breaches that are accidental and unintentional. Educating employees about the importance of observing security policies is one of most important processes. In addition following guidelines can help to enforce security policies.

2.15.1 Increasing Awareness

A security policy is only successful if employees understand and regularly observe the procedures. Those in charge of corporate security must understand the level of employee awareness in order to determine whether security policies are effective. Conducting a survey can help you determine this level and take steps to raise awareness, if necessary. Some of the questions such a survey might include are:

- Do employees know that there are security policies?
- Do they know where to find them?
- Are the policies easily accessible?

- Have all the employees read the policies?
- Do the employees understand the policies?

2.15.2 Communicating effectively

Whether explaining security policies to new hires or sharing updates with employees, clear communication through established channels is critical. Making sure that employees understand why they are being asked to comply with security policies is also an important aspect of communication. Additional communications guidelines include:

- Target communications for various user communities.
- Provide a list of policy updates in your annual training.
- Supplement primary communications vehicles with website and newsletter articles.

2.15.3 Simplify enforcement

Convince employees to comply with every policy. Generating a higher level of compliance by creating realistic, workable policies shall help.

- **Creating a manageable number of policies:** Keeping the number of policies manageable so users can more easily find the policy that they need.
- **Making policies understandable for all audiences:** Using language that is suited for all users with examples to illustrate how the user can comply with the policy.
- **Making it easy to comply:** Including employees in policy review process to get some sense of the ease of compliance.
- **Integrating security with business processes:** Integrating security policy compliance into business processes, so employees won't need to bypass security procedures in the process of doing their jobs.
- **Aligning policies with job requirements:** Even well-intentioned policies can get in the way of job requirements.

2.15.4 Integrating security with the corporate culture

Integrating security into the corporate culture helps to convince employees and harried executives that security is central to business success. This approach can foster a feeling of community and encourage everyone to feel that their support of security policies is important.

- **Making employees a partner in the security challenge:** Employees will be more likely to support security initiatives if they feel that the security team is there to help them instead of to police them. Establish good relationships and use the awareness programme to encourage business leaders to drive security within their organisations.
- **Making security policy part of a larger compliance initiative:** Work with human resources, legal, and other compliance teams so that there is importance, credibility, and urgency attached to any policy training or communication.
- **Tying security policies to company's code of business conduct:** Educate employees to understand that their compliance with security initiatives is integral to overall appropriate behaviour and critical to business success.

2.16 Summary

Information Security is a business issue and it needs to be properly integrated into the organisation's overall business goals and objectives because security issues can negatively affect the resources an organisation depends upon. Security management has become more important over the years because networks have evolved from centralised environments to distributed environments. The objectives of Information Security are to provide confidentiality, integrity and availability to data and resources.

2.17 Questions

1. The Primary objective of implementing Information security management is to:
    A. Ensure reasonable security practices
    B. Comply with internal audit requirements
    C. Adopt globally recognized standards
    D. Protect information assets
2. Which of the following is primary function of information security policies?
    A. Align information security practices with strategy
    B. Communicate intent of management to stakeholders
    C. Perform risk assessment of IT operations and assets
    D. Ensure compliance with requirements of standards
3. IT security policies are set of various policies addressing different IT areas based on the IT infrastructure of organisation. Which of the following policy is most common in all organisations?
    A. Acceptable use policy
    B. BYOD policy
    C. Data encryption policy
    D. Biometric security policy
4. Data-Diddling refers to:
    A. Data manipulation
    B. Data entry
    C. Data processing
    D. Data backup
5. Protecting integrity of data primarily focuses on:
    A. Intentional leakage of data
    B. Accidental loss of data
    C. Accuracy and completeness
    D. Data backup procedures

6. Primary function of information security steering committee is to:
   - A. Manage information security
   - B. Select security projects
   - C. Define security policies
   - D. Direct IT security strategy

7. Which of the following is primary reason for periodic review of security policy?
   - A. Compliance requirements
   - B. Changes on board of directors
   - C. Changes in environment
   - D. Joining of new employees

8. Main benefit of Control self-assessment is:
   - A. Replacement of internal audits
   - B. Implement strong controls
   - C. Removal of redundant controls
   - D. User awareness of controls

9. Which of the following is best evidence indicting support and commitment of senior management for information security initiatives?
   - A. Directive for adopting global security standard
   - B. Higher percentage of budget for security projects
   - C. Assigning responsibilities for security to IT head
   - D. Information security is on monthly meeting agenda

10. Which of the following is a concern for compliance with information security policy?
    - A. Decrease in low risk findings in audit report
    - B. High number of approved and open policy exceptions
    - C. Security policy is reviewed once in two years
    - D. Security policy is signed by chief information officer

2.18 Answers and Explanations

1. D. The primary objective of information security management is to provide adequate level of protection to information security assets.

2. B. Policies are vehicle to communicate management's intent to all stakeholders. Information security practices are aligned with business objectives and not the strategy. Security policies are defined as outcome of risk assessment. Compliance with standard is not primary function of policies.

3. A. Acceptable use policy that address the use of IT assets by users is most common in all organisations that depends upon IT. Policies in other option depend upon organisation's use of BYOD or Encryption or Biometric.

4. A. Datas Diddling is the changing of data before or during entry into the computer system with malicious intent.

5. C. Integrity primarily refers to reliability that is achieved by implementing controls to ensure accuracy and completeness of data.

6. D. Primary function of IT security steering committee is to direct and guide IT security within organisation. Other functions can be delegated.

7. C. Changes in environment introduce new risks. In order to address them it is necessary to review the security policy based on assessment of new risks. Other options are secondary reasons.

8. D. Main benefit of control self-assessment is process owners are aware of risks and threats impacting desired outcome of process since they are asked to select and evaluate the controls.

9. D. Without senior management's support security cannot be a success. There are many activities senior management is involved in effective security initiative. Reviewing progress of security in monthly meeting is one of them. Other options may or may not indicate unless there is more evidence to conclude.

10. B. Policy exceptions are temporary and must be reviewed and closed as per plan. Increasing number of exceptions indicates that the policy provisions may not be appropriate and hence need to be reviewed. Other options are not concerns.

CHAPTER 3: INFORMATION ASSETS AND THEIR PROTECTION

3.1 Introduction

Effective control requires a detailed inventory of information assets. Such a list is the first step in classifying the assets and determining the level of protection to be provided to each asset. The inventory record of each information asset should include:

- Specific identification of the asset: Server, printer, network device etc.
- Relative value to the organisation (based on the impact on business in case of compromise. Many times this value is determined based on the class of information processes/stored by the asset)
- Location: Where the asset is located? Depending on class of information location and protection might be decided
- Security/risk classification
- Asset group (where the asset forms part of a larger information system)
- Owner
- Designated custodian

Information is the major business driver for almost all organisations. Dependence on information technology to collect, process and store this information to execute business operations requires that the information must be appropriately protected. Organisations cannot think of protecting entire data and information within organisation uniformly. The reason is there are set of information that organisation want to: 1. Publish 2. Share with select entities and business partners 3. Made available to internal users and stakeholders 4. Should not be known for more than select few. A uniform protection may introduce unnecessary delay and sometimes create challenges for operations. The solution organisation adopt is known identify the information that needs various levels of protection and put them in appropriate “bucket”. Now the bucket can be protected as per nature of information it contains.

Information Asset and protection guideline helps information owners in developing and implementing a comprehensive risk-based strategy for information assets protection. Key strategies are:

- Defining policy, schema and guidelines for classifying and labelling information,
- Defining levels of protection during every stage of information life cycle i.e. collecting, storing, using, processing, transmitting, and disposing,
- Educating users and owners of information on classification schema and protection levels
- Including information breach incidents in incident management process
- Review, audit/compliance processes.

The most secure environment for using restricted data files is a standalone workstation: a computer with no wired, wireless, or dial-in/out network connectivity. However in certain circumstances a user might need to connect his workstation to a network in order to access a shared resource such as a secure server, or common database or global information. This chapter covers procedures generally used for improving protection of information assets including data. Users should be aware that maintaining security in a network environment is complex and can requires a systemic approach that can provide a "defence in depth" for organisational information assets. This requires considerable technical knowhow, skill and experience.

3.2 Why Information classification?

'Data' means information held by the company on its own behalf and/or that entrusted to it by others. It is a representation of facts, concepts, or instructions in a formalised manner suitable for communication, interpretation, or processing by humans or by automatic means. It is also information (original or derived) organised for analysis or used to reason or make decisions. The following are examples of the media which may contain or comprise information/data.

- Databases
- Data files
- Back-up media
- On-line magnetic media
- Off-line magnetic media
- Paper
- System documentation
- User manuals
- Training material
- Operational or support procedures
- Continuity plans
- Fall-back arrangements

Information classification can provide organisations with a systematic approach to protecting information consistently across all parts of organisation and for all versions of information (original, copies, discarded, outdated etc.). Information follows a life cycle consisting of one or more of stages such as: origination, draft, approved/signed, received, stored, processed, transmission, archived, discarded, destruction etc. The organisation is expected to protect information, during each stage of its lifecycle in a consistent manner. The state in which information exists can also influence how a piece of information should be protected.

3.3 Benefits from information classification

Table 3.1: Benefits of Information classification

Determines the level of protection to apply to information	
Description	Information classification can help in determining the risk associated in case of loss and thus prevent 'over-protecting' and/or 'under-protecting', ensuring that information is adequately protected (e.g. against unauthorised disclosure, theft and information leakage)

Example	Information classification is used on a joint project with multiple third parties. Classifying information ensures that it is adequately protected during transmission between the third parties and sent only to authorised individuals
Helps to meet compliance requirements	
Description	Information classification can be used to demonstrate that the organisation is meeting particular compliance requirements (e.g. Data Protection and Privacy directives) and regulation (e.g. RBI)
Example	Internal audit uses information classification to identify documents containing Personally Identifiable Information (PII) and determine whether it has been adequately protected
Reduces operational costs	
Description	Information classification helps to ensure that security controls are only applied to information that requires such protection. This can help reduce the demand on resources and staff and ultimately reduce the cost of protecting information
Example	IT operational costs are reduced by encrypting a smaller amount of information, e.g. only information that has been classified and identified as being secret
Enables access control technologies to function more effectively	
Description	Information classification can help enforce access control policies by using the classification label to determine if an individual can gain access to a piece of information (e.g. information labelled as Secret can only be accessed by individuals that have been granted a security clearance of Secret)
Example	The Exchange may choose to deploy an information classification scheme to help ensure that users gain appropriate access to protected files. • **Digital Rights Management Solution (DRM):** Information classification can be used to control access and privileges for each DRM object according to individuals' security clearance (e.g. individuals assigned to work on a particular project may access files classified as secret) • **Records management:** Information classification can be used in records management by facilitating the organisation of information, e.g. according to a particular client, date information was created or specified retention period. • **E-Discovery investigation:** Information classification can be used to identify electronic information in storage that is relevant to a business transaction that has resulted in, or can be expected to give rise to, legal action.

Factors that should be considered when determining the level of confidentiality of information are:

- Changes to the content of information
- Changes to external conditions over time
- Aggregation of individual pieces of information

3.4 Information Classification policy

An information classification policy is one of the critical components of Information Security. An information security classification policy addresses the following:

- Structure of classification schema (categories of classes)
- Information owners and custodians
- Protection levels for each class of information defined by schema
- Classification method using risk management process i.e. depending upon impact on business if information is breached or not available and possibility (Likelihood) of breach.

Policy also determines the accountability of Information owners, custodians and users. Generally owners are responsible for assigning classifications to information assets according to the standard information classification system (schema and method) adopted by the organisation. Where practicable, the information category shall be embedded in the information itself.

3.5 Classification schema

All organisational information and all information entrusted to Company from third parties may fall into one of the following four classifications, presented in order of increasing sensitivity. Most organisations may follow following classes: Top secret, confidential, sensitive, internal and public. The table describes the general description of classification schema, however organisation may adopt different schema depending upon requirement, nature of business, compliance requirements etc.

Information Category	Description	Examples
Unclassified/ Public	Information is not confidential and can be made public without any implications for company.	• Product brochures widely distributed • Information widely available in the public domain, including publicly available company web site areas • Sample downloads of company software that is for sale • Financial reports required by regulatory authorities • Newsletters for external transmission

Information Category	Description	Examples
Sensitive	• Requires special precautions to ensure the integrity and confidentiality of the data by protecting it from unauthorised modification or deletion • Requires higher than normal assurance of accuracy and completeness.	• Passwords and information on corporate security procedures • Know-how used to process client information • Standard Operating Procedures used in all parts of Company's business • All Company-developed software code, whether used internally or sold to clients
Client Confidential Data	Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Client media • Electronic transmissions from clients • Product information generated for the client by company
Company Confidential Data	Information collected and used by Company in the conduct of its business to employ people, to log and fulfil client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Salaries and other personnel data • Accounting data and internal financial reports • Confidential customer business data and confidential contracts • Company business plans

3.6 Data Privacy

Data privacy, also called ***Information Privacy,*** is generally refers to personal information. This personal information can be related to any person or stakeholders who need to provide this information to organisation. For example Banks may have to collect identification proofs, PAN card details, address, telephone numbers from the customers, and generates information like credit cards details, bank account numbers for customers. Or retail stores may collect credit card information from customers. If such information is leaked it may result into identity theft or impersonation by another person with malicious intent. Organisations must take care of protecting such information. Many countries have enacted laws to fix the accountability and organisations must comply with these laws. These laws specifically mandate that organisation must secure personally identifiable information (PII) while processing, sharing with third parties and business associates, users etc.

3.7 Compliance requirements for Private data

There are various compliance requirements related to PersonallyIdentifiable Information or also referred as PII.

1. **PCIDSS: Pay-card industry data security standard:** *De-facto* standard for card related information. Must be complied by all those deals with credit or debit cards which include banks, merchants, intermediately. Although there may not be regulatory or legal requirements as of now for compliance with PCIDSS, it has been accepted by industry.
2. **Information technology Act 2000, (Amendment 2008):** Provides that any organisation is collecting PII shall be liable in case absence of reasonable security of such information results in identify theft.
3. **Reserve Bank and other regulatory authorities like CERT-In, Ministry of IT:** The regulations have mandated processes for collecting, storing, securing data and information including PII. For example one time password (OTP) for online credit card transactions, implementing security processes as per ISO 27001 or equivalent certifiable information security standard etc.
4. Organisations that deals with internationally and collects privacy related information also need to comply with international legislations such as:
    - **Gramm-Leach-Bliley Act:** Mandates how financial institutions must deal with the private information of individuals.
    - **Video Privacy Protection Act:** Prevents wrongful disclosure of an individual's personally identifiable information stemming from their rental or purchase of audio-visual material.
    - **Children's Online Privacy Protection Act (COPPA):** Gives parents control over what information websites can collect from their kids.
    - **Health Insurance Portability and Accountability Act (HIPPA):** Ensures patient confidentiality for all healthcare-related data.
    - **Electronic Communications Privacy Act (ECPA):** Extends government restrictions on wire taps to include transmissions of electronic data.
        a. **Medical Information:** A person may not wish for their medical records to be revealed to others. Revealing medical or psychological conditions or treatments which would be embarrassing. Revealing medical data could also reveal other details about one's personal life.

        b. **Location Information:** As location tracking capabilities of mobile devices are increasing, problems related to user privacy arise. Location data is among the most sensitive data currently being collected.

        c. **Information on World Wide Web:** The ability to control the information one reveals about oneself over the Internet, and who can access that information, has become a growing concern. These concerns include whether e-mail can be stored or read by third parties without consent, or whether third parties can continue to track the web sites someone has visited. Another concern is web sites which are visited collect, store, and possibly share personally identifiable information about users.

3.8 Data Protection

In order to ensure that appropriate protection is provided to information assets organisation must first identify and classify all information assets. Information assets must take place at all levels described below:

- For paper documents, including output from systems, classification will apply to each individual document;
- For server-based systems, classification will be done at the file or data level;
- For information in a database, the classification will normally apply to the entire database;
- For critical databases, classification may apply to column level, at the discretion of the information owner;
- For distributed systems, classification will normally apply to all information supported by the system – in this case the classification is determined by the highest category of information supported;
- CD, DVD, diskettes, tapes, memory cards, USB sticks and any other information carriers should be classified at the highest category of information carried.

Protection policy must be defined based on class of information and type of information described above. Protection level for each class of information shall be determined based on the risk to organisation due to breach of such information. While formulating data protection levels organisations need to consider these key points:

1. Physical security to all assets involved in information lifecycle:
    a. Desktops/Laptops
    b. Servers/storage area networks (SAN)
    c. USB, tapes, DVDs and other Potable storages
    d. Documents
2. Physical security of back-up media during transition depending upon the criticality of contents
3. Strong room/Safe, lock and key, fireproof cupboards for paper documents and other portable storages based on class of information.
4. Strong access controls based on principle of “Need to know and need to do”. Information asset owner/custodian may consider defining access control matrix for approving and granting accesses to information based on class.
5. Encryption of information during transmission, processing and storing.
6. Content management process for data being published (printed, advertisement, website), transmitted, communicated, mailed.
7. Information communication policies and approval process, if required, before accessing/processing/transmitting classified information.
8. Consider automating data protection process based on cost-benefit analysis
9. Monitoring outgoing traffic particularly for classified information.

Note: Various protection controls mentioned here are discussed in respective modules/chapters e.g. Network security and encryption is discussed in Module 1, access controls are discussed on Chapter 5 and physical and environmental security is discussed in Chapter 4.

3.8.1 Data Protection automation and challenges in automation

Organisation considering protecting data using automated tools finds it difficult to get appropriate information due to confusion in the marketplace (vendor) regarding DLP (data loss prevention) controls. Although there are many factors, most notable are a general lack of understanding in the vendor community about what constitutes risk to a business and bottlenecks due to impractical processes.

Organisations want to protect confidential data and also have to comply with laws and regulations look for technology to offer quick solution. However most important thing to realise is that it's not the technology, it's the methodology and execution strategy that governs the results. Organisation's requirements for data protection can be categorised as:

1. Protecting data from leaking out of organisation through mail and internet (Network)
2. Controlling leakage of data using removable media (End Point)
3. Protecting data stored on storage networks (NAS/SAN)

Considering these requirements organisations may have to look for multiple technological solutions. The solutions generally referred under popular acronym DLP (Data leak prevention/ Data loss prevention/Data leak protection) provide few capabilities to be implemented independently e.g. there are solutions that focuses on protecting data passing through networks based on the rule-set and classification. Another component that focuses on endpoint controls based on rules and classification.

In addition there are solutions referred by acronym DRM (Digital rights Management) that can be applied to data files. The solutions expects creator of data file to decide who shall access the data and need to add in central user list. Sometimes this becomes impractical when such files are meant for users out of organisation and they need to be authenticated by DRM server. Another challenge is that not all products support all types of data files. (E.g. Microsoft format, PDF, JPG etc.)

The third solution has acronym DAM (Digital Access Management) that works at data base level and manages the access rights while providing data to applications, based on rules and classification. A prerequisite for successful implementation of these tools is appropriate rule set and data classification based on impact of risks associated with data leak. Following steps might be useful:

- Create an information risk profile based on impact severity
- Create awareness about risk associated with data leak
- Define and establish process for data classification
- Identify information resources and determine classification
- Determine rule set for data usage and movement based on class of data
- Identify solutions that meets organisation's requirements
- Integrate controls into the rest of the organisation

3.9 Classification of other Information Assets

Classification of Information Assets helps an organisation address their most significant risks, by affording them the appropriate level of security. As all information does not have the same value or use, or is subject to the same risks their protection mechanisms, recovery processes, etc., are different, with differing costs associated with them. Information assets other than data can be, categorised into following types:

1. **Servers:** Servers are the most physically secure class of systems. This is due to the common practice of placing them in a location that has better access and environmental control. Although this class may be the most physically secure, their overall security is dependent on the physical security of the workstations and portable devices that access them.
2. **Workstations:** Usually located in more open or accessible areas of a facility. Because of their availability within the workplace, workstations can be prone to physical security problems if used carelessly.
3. **Portable devices:** Can be an organisation's security nightmare. Although issuing laptops and PDAs to employees facilitates flexibility and productivity in an organisation, it poses several serious risks with regard to physical security. Besides, more and more organisations are adopting Bring Your Own Device (BYOD) policy which further makes the portable device and the corporate network vulnerable. With users accessing the company's internal information systems from anywhere, a breach in physical security on one of these devices could undermine an organisation's information security. Extreme care must be taken with this class.
4. **Printers:** Although the data is stored on electronic for the purpose. The reports, letters, communications etc. have to be printed. Organisations deploy printers. In order to optimise use of printer most organisations deploy network based printers shared among group of users. In such situation it is necessary to control the number of copies printed particularly if the information is classified and the owner is not attending the printer, there is possibility that unauthorised users may access such reports.
5. **Network devices:** Devices deployed for establishing communication which includes routers, switches, firewalls, cables, wireless devices and other network monitoring tools.

Unattended equipment: Special care must be taken to protect the unattended devices. For example telecom companies may install towers to facilitate mobile communication that are not attended. Or Bank installing ATM without security guards.

3.10 Privacy management issues and role of IS Auditors

One of the many challenging and formidable risk management issues faced by organisations today is protecting the privacy of customers and employees personal information. The organisation's customers, suppliers, and business partners want assurances that personal information collected from them is protected and used only for the purposes for which it was originally collected. When privacy is managed well, organisations earn the trust of their customers, employees, and other data subjects. When it's managed poorly, trust and confidence quickly erode. Privacy definitions in the business environment vary widely depending on country, culture, political environment, and legal framework. In many countries, privacy is closely linked to data protection. It can mean freedom from unwanted attention from others or freedom from observation or surveillance. And in today's business context, privacy often refers to the privacy of personal information about an individual and the individual's ability to:

- Know, how his or her personal information is handled.
- Control the information collected.

It is important that the organisation implements an effective privacy programme that includes:

- Privacy governance and accountability
- Written policies and procedures
- Controls and processes
- Roles and responsibilities
- Training and education of employees
- Monitoring and auditing
- Incident response plans
- Plans for responding to detected problems and corrective action

An organisation's governing body is responsible for establishing an appropriate privacy framework, and internal auditing can evaluate that framework, identify significant risks, and make appropriate recommendations.

When evaluating an organisation's privacy framework, internal auditors should consider the following:

- Laws and regulations in all jurisdictions in which business is conducted
- Internal privacy policies and guidelines
- Liaising with in-house legal counsel to understand legal implications
- Liaising with information technology specialists and business process owners to understand information security implications
- The maturity of the organisation's privacy controls

The auditor's role includes conducting privacy risk assessments and providing assurance over privacy controls across the organisation

Typical areas that internal auditing may review include:

- Management oversight
- Privacy policies and controls
- Systems that process personal information
- Data collection methodologies
- Uses of personal information according to stated intent, applicable laws, and other regulations
- Security practices covering personal information

Privacy Management audit normally includes the following:

- Is private information being disposed of according to policy and procedures?

- Is the privacy programme supported by the corporate culture?
- Are workstations locked when unattended?
- Are documents stored securely prior to disposal or shredding?
- Are working documents with private data stored securely?
- How effective are the organisation's privacy awareness and training programmes?

3.11 Summary

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorised access, use, disclosure, destruction, modification, or disruption or distribution. The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, documentation, and review. This makes information security an indispensable part of all the business operations across different domains. The objective of security is to ensure confidentiality, integrity and availability company information. Information Security Policies can be issue-specific and system-specific. Security management should work from the top down, from senior management down to the staff.

3.12 Questions

1. Which of the following is Primary purpose of Information classification?
    - A. Comply with regulatory requirement
    - B. Assign owner to information asset
    - C. Provide appropriate level of protection
    - D. Reduce costs of data protection
2. Data base administrator (DBA) is:
    - A. Information Custodian
    - B. System Administrator
    - C. End User
    - D. Data Owner
3. Effectiveness of information Security awareness training programme is best indicated by increase in:
    - A. Percentage of classified and labelled information
    - B. Number of mails with attachments
    - C. Number of incidents reported by users
    - D. Percentage of contract employees

4. Classification of information is primarily based on:

   A. Where the information is stored?

   B. Who has access to information?

   C. What will happen if information is not available?

   D. Why attachments to mail are encrypted?

5. Which of the following best helps in classifying the information within organisations?

   A. Using minimum classes in classification schema

   B. Conducting training on classification schema

   C. Labelling all information based on classification schema

   D. Determining storage based on classification schema

6. A business application is hosted on a server. Being a small application the database required the application is also on the same server. Which of the following is best way to determine the class of the server?

   A. All servers are critical assets for organisation

   B. Based on classification of application hosted

   C. Same as class of database decided by business

   D. As decided by data base administrator (DBA)

7. Which of the following is a major threat related to private data of customers collect by the organisation?

   A. Loss of data

   B. Integrity of data

   C. Data diddling

   D. Identify theft

8. Which of the following controls can be implemented effectively due to classification of data?

   A. Input validation

   B. Access controls

   C. Scanning for viruses

   D. Internal audit

9. While determining appropriate level of protection to information asset, IS auditor should PRMARILY focus on which of the following evidence?

   A. Results of risk assessment

   B. Relative value to business

   C. List of users having access

   D. Classification of asset

10. Which of the following is PRIMARY consideration for classifying information assets? Assets to be classified based on:

    A. Level of protection provided.

    B. Inputs by data owner.

    C. Result of risk analysis.

    D. Requirements of security policy.

3.13 Answers and Explanations

1.C Primary purpose of information classification is to provide appropriate level of protection to information assets.

2.A. DBA is an Information custodian as DBA is responsible for maintaining database but do not have right to modify the data.

3. A. Security awareness programme helps users and employees to understand reason for security and help in implementing it effectively. Options B, C and D do not provide information on improvement aspect.

4. C. It helps in assessing the risks associated and determine the protection level i.e. class of information. A, B and D are determined based on classification.

5. B. Training users on how to classify information as per definition provided in classification schema shall best help users in classifying the information. A. Number of classes shall depend upon organisation's objectives. C and D are performed after classification of information.

6. C. The primary asset in this case is data that is being stored and process by the application. The server supports the data and hence must be classified as per the classification of database owned by business function.

7.D. Misuse of customer's private data can result in identity theft resulting in making organisation liable for losses and might affect reputation adversely. A, B and C are threats can be managed by internal controls.

8. B. Information classifications help management in implementing better access controls for sensitive information. Other controls are not related to data classification.

9. A. Appropriate level of protection to asset is determined based on risk associated with asset based on vulnerabilities. Results of risk assessment, therefore is primary information IS auditor should review. Relative value of asset to business is considered while assessing impact of risk associated. Access to asset is determined based on classification of asset and need to do basis which is determined based on risk associated. Assets are classified based on result of risk assessment.

10. C. Assets must be primarily classified based on risk associated. Level of protection is to be decided based on result of risk analysis and not the other way round. Inputs from the owner are useful in assessing risk for the organisation. Security policy provides intent of management however the policies are based on result of risk analysis.

CHAPTER 4: PHYSICAL AND ENVIRONMENTAL CONTROLS

4.1 Introduction

Prior to use of computers and communications technology most business assets were in physical form and securing them was primarily controlled manually. However technology has also enabled attackers to launch successful attack without being physically near the victim organisation. Apart from traditional requirement of security organisation's assets, physical security also focuses on securing technology assets physically. Physical security of computers and related resources was not as challenging in earlier days as it is today, because computers were mostly mainframes that were locked away in server rooms, and only a few people knew what to do with them anyway. Today, there is a computer on almost every desk, and access to devices and resources is spread throughout the environment. Besides, organisations have several remote and mobile users. Properly protecting these computer systems, networks, facilities, and employees has become an overwhelming task to many organisations.

Use of technology has also added a requirement to ensure that the environmental controls are in place so that the technology deployed can perform as expected. For example computer uses electrical energy to process, store and transmit data. In the process they generate heat. This heat can affect the small electronic circuits within computers resulting in failure of technology to perform. This means the environment must be able to provide sustain climatic conditions like uniform low temperature, dust free air with lower level of humidity.

Physical security should be implemented as part of layered approach to security so that if one layer fails there are other layers to protect the information and other valuable assets. A physical security programme should comprise ***safety*** and ***security*** mechanisms. Safety mechanisms should cover the protection of life and assets against fire, natural disasters, and devastating accidents. Security mechanisms should cover theft, vandalism and attacks by individuals.

4.2 Physical security controls

Physical security is a term in computer security that refers to the ability of people to physically gain access to a computer system. These can be enforced by personnel such as a border guard, a doorman, a ticket checker, etc., or with a device such as a turnstile (a gate which ensures one-way traffic of people). There may be fences to avoid circumventing this access control. An alternative of access control in the strict sense (physically controlling access itself) is a system of checking authorised presence, see e.g. Ticket controller (transportation).

Physical control can be achieved by a human (a guard, bouncer, or receptionist), through mechanical means such as locks and keys, or through technological means such as access control systems like the access control vestibule. Within these environments, physical key management may also be employed as a means of further managing and monitoring access to mechanically keyed areas or access to certain small assets.

Access control is the ability to permit or deny the use of a particular resource by a particular entity. Access control mechanisms can be used in managing physical resources (such as a movie theatre, to which only ticketholders should be admitted), logical resources (a bank account, with a limited number of people authorised to make a withdrawal), or digital resources (for example, a private text document on a computer, which only certain users should be able to read).

4.2.1 Objectives of physical access controls

Physical access control is a matter of who, where, and when. An access control system determines who is allowed, where they are allowed, and when they are allowed to enter or exit. Physical Access controls seek to safeguard the IS resources from physical access exposures. However designing, acquiring and implementing these controls is an expensive proposition.

i. Physical access controls encompass securing physical access to computing equipment as well as facilities housing the IS computing equipment and supplies. The choice of safeguard should be such that they prevent unauthorised physical access but at the same time cause the least inconvenience to authorized users.

ii. Physical access controls restrict physical access to resources and protect them from intentional and unintentional loss or impairment. Assets to be protected could include:

    - Primary computer facilities
    - Cooling system facilities
    - Microcomputers
    - Telecommunications equipment and lines, including wiring closets Sensitive areas such as buildings, individual rooms or equipment.

iii. Physical access controls may include – manual door or cipher key locks, photo IDS and security guards, entry logs, perimeter intrusion locks etc. The effectiveness of these controls is to:

    - Grant/discontinue access authorisations.
    - Control passkeys and entry during and after normal business hours.
    - Handle emergencies.
    - Control the deposit and withdrawals of tapes and other storage media to and from the library.

iv. Physical controls should also include:

    - Pre-planned appointments.
    - Identification checks.
    - Controlling the reception area.
    - Logging in visitors.
    - Escorting visitors while in sensitive areas etc.

4.2.2 Physical Security Threats and Exposures

One of the most important steps in any risk management procedure is to identify the threats to any organisation. A threat is defined as an event (for example- a theft, fire accident etc.), the occurrence of which can have an adverse impact on the well-being of an asset. Physical threats to information system assets comprises of threats to computing equipment, facilities which house the equipment, media and people. This section deals with the security of the physical equipment and infrastructure and the environment in which they operate. The focus of the IS Auditor is to examine all factors that adversely bear on the confidentiality, integrity and availability of the information, due to improper physical access. Confidentiality, Integrity and Availability (CIA Triad) are the core principles of information safety.

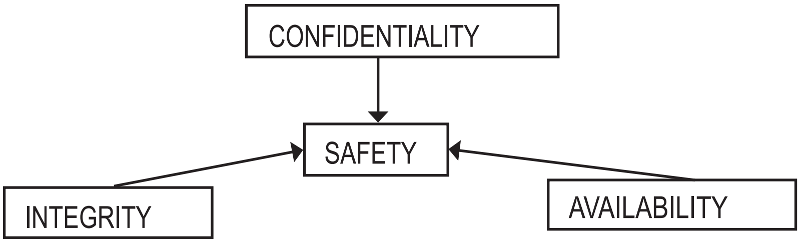


Figure 4.1: Principles of Information Safety

Confidentiality: Preventing disclosure of information to unauthorised individuals or systems.

Integrity: Prevent modification of data by unauthorised personnel.

Availability: Information must be available when it is needed.

Physical security threats can be placed into four major categories:

i. **Electrical:** Electrical vulnerabilities are seen in things such as spikes in voltage to different devices and hardware systems, or brownouts due to an insufficient voltage supply. Electrical threats also come from the noise of unconditioned power and, in some extreme circumstances like total power loss.

ii. **Environmental:** Not only do you need to secure your systems from human interference, but also need to secure them from the interference of natural disasters such as fires, hurricanes, tornados, and flooding, which fall under the realm of environmental threat. Extreme temperature and humidity are also environmental issues.

iii. **Hardware:** It has the threat of physical damage to corporate hardware or its theft.

iv. **Maintenance:** These threats are due to poor handling of electronic components, which cause ESD (electrostatic discharge), the lack of spare parts, poor cabling, poor device labelling, etc.

4.2.3 Sources of Physical security threats

The sources of physical access threats can be broadly divided into the following based on the nature of access. The perpetrators or source of physical threats can be as follows:

- Physical access to IS resources by unauthorised personnel.
- Authorised personnel having pre-determined rights of access, misusing their rights in a manner prejudicial to the interests of the organisation.
- Authorised personnel gaining access to Information Systems resources in respect of which they are not authorised access. (i.e. gaining access to resources beyond their rights of “need to know; need to do”)

- Interested or Informed outsiders such as competitors, thieves, organised criminals and hackers
- Former Employees/outsourced agencies former employees
- Accidental/Ignorant who unknowingly perpetrates a violation
- Discontented or disgruntled employees. Outsourced agencies employees
- Employees on strike or issues at outsourced agency
- Employees under termination or suspended and pending termination
- Addicted to substances or gamblers
- Experiencing financial or emotional problems

Threats from improper physical access usually are human-induced. Some examples are:

- Unauthorised persons gaining access to restricted areas. Examples are prospective suppliers gaining access to computer terminal of purchases department, thereby viewing list of authorised suppliers and rates being displayed on the screen during data entry.
- Employees gaining access to areas not authorised, e.g. sales executives gaining access to server room.
- Damage, vandalism or theft of equipment or other IS resources.
- Abuse of data processing resources, e.g. employees using internet for personal purposes.
- Damage due to civil disturbances and war.
- Embezzlement of computer supplies, e.g. floppies, cartridges, printer consumables.
- Public disclosure of sensitive information, e.g. Information regarding location of servers, confidential or embarrassing information.

4.2.4 Physical access exposures to assets

(i) **Unintentional or Accidental:** Authorized personnel or unauthorised personnel unintentionally gaining physical access to IS resources result in accidentally or inadvertently causing loss or damage to the organisation.

(ii) **Deliberate:** Unauthorised personnel may deliberately gain access or authorized personnel may deliberately gain access to IS resources, for which they are not permitted or possess rights of access. This may result in the perpetrator achieving his objective of causing loss or damage to the organisation or gain personal monetary benefits or otherwise.

(iii) **Losses:** Improper physical access to IS resources may result in losses to organisation which can result in compromising one or any of the following:

- **Confidentiality** of organisational information or knowledge of protected organisational resources. Example: unauthorised access to systems containing sensitive information may be viewed or copied by visitors accidentally gaining access to such systems.
- **Integrity** of information by improper manipulation of information or data contained on systems or media. Example: Unauthorised access to record rooms or databases may result in modification or deletion of file content.

- **Availability** of information. Improper access to IS resources may be used to adversely impact availability of IS resources' ultimately preventing or delaying access to organisational information and business applications. Example: A disgruntled bank employee may switch of power to information servers thus sabotaging operations.

4.2.5 Physical Security Control Techniques

In order to provide physical security organisation must plan security controls. This can include:

- Selection of location for hosting infrastructure and technology facilities
- Planning areas for high security requirements (e.g. data centre, executive wing), Medium security requirements (e.g. employee work areas), Low security requirements (e.g., public area, receptions) and other areas where risk cannot be determined but may be prone for launching attack (e.g. parking, loading/unloading areas) Organisation may have more layers based on their specific requirements.
- Define physical security controls and protection levels for each layer

Choosing and designing a secure site

Organizations may consider various controls to implement physical security. In the choice of the location during initial planning for a facility the following concerns are to be addressed.

- **Local considerations:** What is the local rate of crime (such as forced entry and burglary)?
- **External services:** The relative proximity of local emergency services, such as police, fire, and hospitals or medical facilities is to be factored in while choosing a site.
- With respect to designing the site the following considerations apply:
- **Visibility:** Facilities such as data centres should not be visible or identifiable from the outside, that is, no windows or directional signs.
- **Windows:** Windows are normally not acceptable in a data centre to avoid data leakage through electromagnetic radiation emitted by monitors. If they do exist, however, they must be translucent (semi-transparent, i.e. allowing light without being able to view things clearly) and shatterproof or monitors should not be facing them.
- **Doors:** Doors in the computer centre must resist forcible entry and have a fire rating equal to the walls. Emergency exits must be clearly marked and monitored or alarmed. Electric door locks on emergency exits should revert to a disabled state if power outages occur to enable safe evacuation. While this may be considered a security issue, personnel safety always takes precedence, and these doors should be manned in an emergency.

Security Management

- **Controlled user registration procedure:** It should be ensured that rights of physical access are given only to persons entitled thereto and to the extent necessary, based on the principles of least privileges.

- **Audit Trails.** With respect to physical security, audit trails and access control logs are vital because management needs to know where access attempts occurred and who attempted them. The audit trails or access logs must record the following:
  - o The date-and time of the access attempt
  - o Whether the attempt was successful or not
  - o Where the access was granted (which door, for example)
  - o Who attempted the access
  - o Who modified the access privileges at the supervisor level
- **Reporting and incident handling procedure:** Once an unauthorised event is detected, appropriate procedures should be in place to enable reporting of such incidents and effectively handling such incidents to mitigate losses. The security administrator should be kept notified of such incidents. He may use such history to effect modifications to the security policy.

Emergency procedures

The implementation of emergency procedures and employee training and knowledge of these procedures is an important part of administrative physical controls. These procedures should be clearly documented, readily accessible (including copies stored of-site in the event of a disaster), and updated periodically.

Human resource controls

These includes identification of employees and visitors, providing identity cards, assigning responsibilities, provided training in physical security, monitoring behaviour, escort terminated or resigned/retired employees. Human resources controls may be implemented by various departments including human resource, physical security, facility management etc.

One of most important control is process of providing access cards to employees, vendor personnel working onsite and visitors. The process should aim in preventing generation of false cards, modifying contents of cards, accounting for lost cards and reconciliation of cards to detect missing/lost cards. In addition a process to grant, change and revoke access must be in place.

Perimeter security

i. **Guards:** Guards are commonly deployed in perimeter control, depending on cost and sensitivity of resource to be secured. While guards are capable of applying subjective intelligence, they are also subject to the risks of social engineering. They are useful whenever immediate, discriminating judgment is required.

ii. **Dogs:** Dogs are used in perimeter security, they are loyal, reliable, and have a keen sense of smell and hearing. However, they cannot make judgment calls the way humans can.

iii. **Compound walls and perimeter fencing:** A common method of securing against unauthorised boundary access to the facility. It helps in deterring casual intruders but is ineffective against a determined intruder.

iv. **Lighting:** Lighting is also one of the most common forms of perimeter or boundary protection. Extensive outside lighting of entrances or parking areas can discourage casual intruders.

v. **Deadman Doors:** Also called as Mantrap systems. These are typically used to secure entrance to sensitive computing facilities or storage areas. This technique involves a pair of doors and the space between the doors is enough to accommodate just one person. When a person is to be admitted to the premises, the second or inner door is closed while the first or outer door opens, thus admitting one person in the space between the doors. Once within that space the first door closes and then the second or inner door opens. Such doors reduce the risk of piggybacking, in which an unauthorised person could enter the secured facility by closely following an authorised person which may or may not be monitored by a guard.

vi. **Bolting door locks:** This is the most commonly used means to secure against unauthorised access to rooms, cabins, closets. These use metal locks and keys and access can be gained by any person having physical possession of the key. This is cheap yet a reasonably effective technique, however control over physical custody and inventory of keys is required.

vii. **Combination or Cipher locks:** The most common kind of cipher lock consists of a push button panel that is mounted near the door outside of the secured area. There are ten numbered buttons on the panel. To gain entry, a person presses a four digit number in a particular pre-determined sequence which disengages the levers for a pre-set interval of time. Cipher locks are used where large number of entrances and exits must be usable frequently. Such locks (both cipher and combination) enable resetting the unlocking sequence periodically or as per requirement. One of the most common application of combination locks is the number locks on briefcases.

viii. **Electronic Door Locks:** Such locks may use electronic card readers, smart cards readers or optical scanners. The readers or scanners read the cards and upon the information stored on the card matching with the information pre-stored internally in the reader device, the device disengages the levers securing the door, thus enabling physical access. The advantages of such locks include:

- This technique provides a higher level of security over the previous discussed devices.
- The same device can be used to distinguish between various categories of users.
- Individual access needs can be restricted through the special internal code and sensor devices.
- Restrictions can be assigned to particular doors or to particular hours.
- Duplication of such cards is difficult.
- Card entry can be easily deactivated from a central electronic control mechanism. This is useful in case of cards being lost or for disabling access to terminated employees etc. This also enables easy implementation of changes to security policy.

- The devices may also include various features such as "card swallow" after pre-set number of failed attempts, activating audible alarms, engaging other access areas thus securing sensitive areas or trapping the unauthorised entrant.

ix. **Biometric Door Locks:** These are some of the most secure locks since they enable access based on individual features such as voice, fingerprint, hand geometry, retina or iris. These are similar to the electronic door locks but more sophisticated since in this case the mechanical component securing the physical door is engaged/disengaged is controlled by an electronic device. In this case the device has a scanner/reader which reads the fingerprint or such other biometric and matching the individuals features with that internally stored.

While these devices are considered highly secure, they suffer from the following disadvantages:

- Relatively high cost of acquisition, implementation and maintenance, hence they are used mainly to secure sensitive installations.
- Time consuming process of user registration.
- Privacy issues relating to use of devices like retina and fingerprint scanners.
- High error rates compared to other devices since they may result in a false rejection or more critically a false acceptance.

Biometric devices can be used for logical access also more about biometric devices is discussed in next section.

(i) **Perimeter intrusion detectors** – The two most common types of physical perimeter detectors are based either on photoelectric sensors or dry contact switches.

  o **Photoelectric sensors** – Photoelectric sensors receive a beam of light from a light-emitting device, creating a grid of either visible white light, or invisible infrared light. An alarm is activated when the beams are broken. The beams can be physically avoided if seen; therefore, invisible infrared light is often used.

  o **Dry contact switches** – Dry contact switches and tape are probably the most common types of perimeter detection. This can consist of metallic foil tape on windows or metal contact switches on doorframes to detect when a door or window has been opened.

x. **Video Cameras:** Cameras provide preventive and detective control. Closed-Circuit Television (CCTV) cameras have to be supplemented by security monitoring and guards for taking corrective action. The location of such cameras and recording/retention of tapes/images for future playback should be decided based on security strategy.

xi. **Identification badges:** Special identification badges such as employee cards, privileged access pass, visitor passes etc. enable tracking movement of personnel. These can also be cards with signature and/or photo identity. These are physically examined by security staff to permit/deny access and detect unauthorised access.

xii. **Manual Logging:** All visitors to the premises are prompted to sign a visitor's log recording the date and time of entry/exit, name of entrant, organisation, purpose etc. The visitor may also be required to authenticate his identity by means of a business card, photo identification card, driver's licence etc.

xiii. **Electronic Logging:** Electronic card users may be used to record the date and time of entry/exit of the card holder by requiring the person to swipe the card both time of entry and exit. This is a faster and more reliable method for restricting access to employees and pre-authorized personnel only. These devices may use electronic/biometric security mechanisms.

xiv. **Controlled single point access:** Physical access to the facility is granted though a single guarded entry point. Multiple entry points may dilute administration of effective security. This involves identifying and eliminating or disabling entry from all entry points except one.

xv. **Controlled Visitor access:** A pre-designated responsible employee or security staff escorts all visitors such as maintenance personnel, contract workers, vendors, consultants for a specified time period (unless they are long-term, in which case guest access may be provided) and auditors.

xvi. **Bonded Personnel:** This is useful in situation where physical access to sensitive facilities is given to employees or outsiders such as contract employees. Bonding (contractors or employees being required to execute a financial bond) such personnel does not improve physical security but only reduces financial impact due to improper access/misuse of physical access.

xvii. **Wireless Proximity Readers:** A proximity reader does not require physical contact between the access card and the reader. The card reader senses the card in possession of a user in the general area (proximity) and enables faster access.

xviii. **Alarm Systems/Motion detectors:** Alarm systems provide detective controls and highlight security breaches to prohibited areas, access to areas beyond restricted hours, violation of direction of movement e.g. where entry only/exit only doors are used. Motion detectors are used to sense unusual movement within a predefined interior security area and thus detect physical breaches of perimeter security, and may sound an alarm.

Device level security: Organisations may also consider security controls that are implemented at device levels:

xix. **Secured Distribution Carts:** One of the issues in batch output control is to get the printed hardcopy reports (which may include confidential materials) securely across to the intended recipients. In such cases distribution trolleys with fixed containers secured by locks are used, the keys to the relevant container are held by the respective user team.

xx. **Cable locks:** A cable lock consists of a plastic-covered steel cable that chains a PC, laptop or peripherals to the desk or other immovable objects.

xxi. **Port controls:** Port controls are devices that secure data ports (such as a floppy drive or a serial or parallel port) and prevent their use.

xxii. **Switch controls:** A switch control is a cover for the on/off switch, which prevents a user from switching of the file server's power.

xxiii. **Peripheral switch controls:** These types of controls are lockable switches that prevent a keyboard from being used.

xxiv. **Biometric Mouse:** The input to the system uses a specially designed mouse, which is usable only by pre-determined/pre-registered person based on the fingerprint of the user.

xxv. **Laptops Security:** Securing laptops and portables represent a significant challenge, especially since, loss of laptops create loss of confidentiality, integrity and availability. Cable locks, biometric mice/fingerprint/iris recognition and encryption of the file system are some of the means available to protect laptops and their data.

Smart Cards

A smart card used for access control is also called a security access card. This card comprises the following types:

- **Photo-image cards:** Photo-image cards are simple identification cards with the photo of the bearer for identification.
- **Digital-coded cards:** Digitally encoded cards contain chips or magnetically encoded strips (possibly in addition to a photo of the bearer). The card reader may be programmed to accept or deny entry based on an online access control computer that can also provide information about the date and time of entry. These cards may also be able to create multi-level access groupings.
- **Wireless proximity readers:** A proximity reader does not require the user to physically insert the access card. This card may also be referred to as a wireless security card. The card reader senses the card in possession of a user in the general area (proximity) and enables access.

4.2.6 Biometric devices

Biometric access control devices are technical applications in physical security. Biometric technologies can be used for identification or authentication. The following are typical biometric characteristics used to uniquely identify or authenticate an individual:

- Fingerprints
- Retina scans
- Iris scans
- Facial scans
- Palm scans
- Hand geometry
- Voice
- Handwritten signature dynamics

Understanding Biometrics

Biometrics is used for identification in physical access control, and for authentication in technical (logical) access control. In biometrics, identification is a one-to-many search of an individual's characteristics from a database of stored images. Authentication in biometrics is a one-to-one search to verify a claim to an identity made by a person. The three main performance measures in biometrics are:

1. **False rejection rate (FRR), or Type I error:** The percentage of valid subjects that are falsely rejected

2. **False acceptance rate (FAR), or Type II error:** The percentage of invalid subjects that are falsely accepted. FAR is more critical than FRR.

3. **Crossover error rate (CER):** The per cent at which the FRR equals the FAR. In most cases, the sensitivity of the biometric detection system can be increased or decreased. If the system's sensitivity is increased, such as in an airport metal detector, the system becomes increasingly selective and has a higher FRR. Conversely, if the sensitivity is decreased, the FAR will increase.

Other important factors that must be evaluated in biometric systems are *enrolment time, throughput rate,* and *acceptability.*

- *Enrolment time* is the time it takes to initially register with a system by providing samples of the biometric characteristic to be evaluated.
- An acceptable enrolment time is around two minutes.
- The *throughput rate* is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a system. Acceptable throughput rates are in the range of 10 subjects per minute.
- *Acceptability* refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system.

4.2.7 Auditing Physical Access Controls

Auditing physical access requires that the auditor to review the physical access risks and controls to form an opinion on the effectiveness of these controls. This involves risk assessment, review of documentation and testing of controls.

i. **Risk Assessment:** The auditor should satisfy himself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures.

ii. **Controls Assessment:** The auditor based on the risk profile evaluates whether physical access controls are in place and adequate to protect the IS assets against the risks.

iii. **Review of Documentation:** Planning for review of physical access controls requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list, cabling diagrams.

iv. **Testing of Controls:** IS auditor should review physical access controls for their effectiveness. This involves:

   - Tour of organisational facilities including outsourced and offsite facilities
   - Physical inventory of computing equipment and supporting infrastructure
   - Interviewing personnel can also provide information on the awareness and knowledge of procedures
   - Observation of safeguards and physical access procedures. This would also involve inspection of

- Core computing facilities.
- Computer storage rooms.
- Communication closets.
- Backup and Off-site facilities.
- Printer rooms.
- Disposal yards and bins.
- Inventory of supplies and consumables.

Some special considerations also involve the following:

- All points of entry/exit
- Glass windows and walls
- Moveable and modular cubicles
- Ventilation/Air-conditioning ducts
- False Ceiling and flooring panels.

Review of Physical access procedures including user registration and authorisation, special access authorisation, logging, periodic review, supervision etc. Employee termination procedures should provide withdrawal of rights such as retrieval of physical devices such as smart cards, access tokens, deactivation of access rights and its appropriate communication to relevant constituents in the organisation. Examination of physical access logs and reports includes examination of incident reporting logs and problem resolution reports.

Some examples of Physical Control Techniques and their suggested audit procedures are given in the table here.

Control Activities	Control Techniques	Audit Procedures
Physical safeguards to commensurate with the risks of physical damage or access.	Identify facilities housing sensitive and critical resources. Identify all threats to physical well-being of sensitive and critical resources are being adequately secured using keys, alarm systems, security devices and other access control devices, including - Use of badges. - Display and output devices. - Data transmission lines. - Power equipment and poser cabling. - Mobile or portable systems.	Review the physical layout diagram of computer, telecommunications and cooling system facilities. Walk through facilities. Review risk analysis. Review procedures for the removal and return of storage media from and to the library. Review of written emergency procedures. Observe a fire drill.

Control Activities	Control Techniques	Audit Procedures
	All deposits and withdrawals of tapes and other storage media from the library are authorized and logged. Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc.	Review the knowledge and awareness of emergency procedures by employees with respect to facilities using interviews, questionnaires etc.
Establish adequate security at entrance and exists based on risk	All employee access is authorized and credentials (badges, ID cards, smart cards) are issued to allow access.	Review procedures and logs of employee entry and exists during and after normal business hours.
	Management conducts regular reviews of individuals with physical access to sensitive facilities.	Review Procedures used by management to ensure that individuals having access to sensitive facilities are adequately restricted and posses' physical access authorization.
	Visitors to the sensitive areas, such as the main computer room and tape/ media library, are formally signed in and escorted.	Review visitor entry logs. Interview guards at the facility entry.
	Entry codes are changed periodically.	Review documentation on logs of entry, code changes and system maintenance.
Perimeter Security	Control/restrict vehicle and pedestrian traffic with measures like fences, gates, locks, guard posts and inspections.	Assess vehicle and pedestrian traffic around high risk facility.
		Inspect guard procedures and practices for controlling access to facility grounds.
	Installation of closed circuit system with recording and warning alarms - 24 hours.	Inspect the facility surveillance system to assess its capability in protecting the facility.
Security control policies and procedures are documented, approved and implemented by management.	Security control policies and procedures at all levels – – Are document – Address purpose, scope, roles, responsibilities and compliance.	Review security policies and procedures at the enterprise level, system level and process level are aligned with business/enterprise stated objectives.

Control Activities	Control Techniques	Audit Procedures
	- Ensure users can be held accountable for their actions - are approved by management and - Periodically reviewed and updated.	

4.3 Environmental Controls

This section examines the risks to IS resources arising from undesired changes in the environment. Environmental threats to information assets include threats primarily relating to facilities and supporting infrastructure, which house and support the computing equipment, media and people. IS Auditor should review all factors that adversely bear on the confidentiality, integrity and availability of the information, due to undesired changes in the environment or ineffective environmental controls.

4.3.1 Objectives of Environmental Controls

The objects to be protected in an environment are much the same as discussed in the section on physical access controls. However from the perspective of environmental exposures and controls, information systems resources may be categorised as follows, with the focus primarily on facilities which house:

i. **Hardware and Media:** Includes Computing Equipment, Communication equipment, and Storage Media

ii. **Information Systems Supporting Infrastructure or Facilities:** This typically includes the following:

- Physical Premises, like Computer Rooms, Cabins, Server Rooms/Farms, Data Centre premises, Printer Rooms, Remote facilities and Storage Areas
- Communication Closets
- Cabling ducts
- Power Source
- Heating, Ventilation and Air Conditioning (HVAC)

iii. **Documentation:** Physical and geographical documentation of computing facilities with emergency excavation plans and incident planning procedures.

iv. **Supplies:** The third party maintenance procedures for say air-conditioning, fire safety, and civil contractors whose entry and assess with respect to their scope of work assigned are to be monitored and logged.

v. **People:** The employees, contract employees, visitors, supervisors and third party maintenance personnel are to be made responsible and accountable for environmental controls in their respective information processing facility (IPF). Training of employees and other stake holders on control procedures is a critical component

4.3.2 Environmental Threats and Exposures

Undesired or unintentional or intentional alteration in the environment in which computing resources function can result in threats to availability of information systems and integrity of information. Exposures from environmental threats include total or partial loss of computing facilities, equipment, documentation and supplies causing loss or damage to organisational data and information and more importantly people. The threats can be broadly classified as Natural and Man-made.

Natural Threats.

Threats to facilities and environment from natural causes can significantly and adversely impact the availability, integrity and confidentiality of information. Examples include:

- Natural disasters such as earthquakes, foods, volcanoes, hurricanes and tornadoes
- Extreme variations in temperature such as heat or cold, snow, sunlight, etc.
- Static electricity
- Humidity, vapours, smoke and suspended particles
- Insects and organisms such as rodents, termites and fungi
- Structural damages due to disasters

Man-made Threats

Human induced threats again can be unintentional or intentional, examples of which are:

- Fire due to negligence and human action
- War Action and Bomb threats
- Power – uncontrolled/unconditioned power, spikes, surges, low voltage
- Equipment failure
- Failure of Air-conditioning, Humidifiers, Heaters
- Food particles and residues, undesired activities in computer facilities such as smoking.
- Structural damages due to human action/inaction and negligence
- Electrical and Electromagnetic Interference (EMI) from Generators, motors.
- Radiation
- Chemical/liquid spills or gas leaks due to human carelessness or negligence

Exposures

Some examples of exposures from violation of environmental controls:

- A fire could destroy valuable computer equipment and supporting infrastructure and invaluable organisational data. Usually the use/storage of thermo coal or Styrofoam (technically called Expanded Polystyrene) material, inflammable material used for construction of the server cabin, false ceiling aggravate the probability of fire and loss due to fire.

- Magnetic tapes use materials which are inflammable.
- Poor quality of power cables can over-heat and cause fire.
- Lightning may burn up communication devices and computing equipment due to improper earthing or grounding.
- Continuous process systems bear the risk of internal component damage due to improper air conditioning or high humidity.
- Damage of keyboards and other computing devices due to accidental dropping of beverages, liquid, etc.
- The organisational policies do not check the consumption of food, tobacco products near computer equipment resulting in food particles leftover in computer facilities that attract rodents, insects which can damage cabling, hard disks.
- Chemical or liquid spills from a nearby unit may seep into the IPF (Information Processing Facility) thereby damaging equipment.
- Sudden surges in power or other voltage fluctuations can irreversibly damage computer equipment.
- Fungi formation on tapes can leads to tapes and disks being not readable.
- EMI (Electromagnetic Interference) from generators can damage integrity of contents on magnetic media.
- Water leakages can induce shocks and short circuits.

Other form of power degradations includes:

a. **Blackout:** It is a complete loss of commercial power.

b. **Sag/dip:** It is a short period of low voltage. The duration is usually for a few seconds. Most voltage sags originate from within the facility; they can be caused by starting an electrical motor that requires a large amount of power, loose or defective wiring, or faults or short circuits. They can also originate from the power company by faults on distant circuits or voltage regulator failures.

c. **Surge:** Surge is a sudden rise in voltage in the power supply. A strong power surge can easily harm unprotected computers and other microprocessor circuits. It also puts a stress on anything else powered by the electric supply, from air conditioning motors to light bulbs.

d. **Transient:** It is line noise or disturbance superimposed on the supply circuit and can cause fluctuations in electrical power.

4.3.3 Techniques of Environmental Controls

The IS supporting infrastructure and facilities not only provide the conducive environment for the effective and efficient functioning of the information processing facility (IPF) but should also protect the contents of such facilities from undesirable variations in the environment. Based on the risk profile, computing equipment, supporting equipment, supplies, documentation and facilities should be appropriately situated, protected to reduce risks from environmental threats and hazards or exposures. Following are list of controls which are to be implemented.

i. Choosing and designing a safe site

The considerations during choosing a location for the facility are (as discussed in the section on Physical Access Controls):

- **Natural disasters:** Probability of natural disasters as compared to other locations? Natural disasters can include weather-related problems (wind, snow, flooding, and so forth) and earthquake faults.
- **Transportation:** Does the site have a problem due to excessive air, highway, or road traffic?
- **External services:** Relative proximity of the local emergency services, such as police, fire, and hospitals or medical facilities are to be factored while choosing a site.

Considerations during designing a site are as follows:

- **Walls:** Entire walls, from the floor to the ceiling, must have an acceptable fire rating. Closets or rooms that store media must have a high fire rating.
- **Ceilings:** Issues of concern regarding ceilings are the weight-bearing rating and the fire rating.
- **Floors:** If the floor is a concrete slab, the concerns are the physical weight it can bear and its fire rating. If it is a raised flooring the fire rating, its electrical conductivity (grounding against static build-up), and that it employs a non-conducting surface material are major concerns. Electrical cables must be enclosed in metal conduit, and data cables must be enclosed in raceways, with all abandoned cable removed. Openings in the raised floor must be smooth and non-abrasive, and they should be protected to minimise the entrance of debris or other combustibles. Ideally, an IPF should be located between floors and not at or near the ground floor, nor should it be located at or near the top floor.
- **Windows:** Windows are normally not acceptable in the data centre. If they do exist, however, they must be translucent and shatterproof.
- **Doors:** Doors in the computer centre must resist forcible entry and have a fire rating equal to the walls. Emergency exits must be clearly marked and monitored or alarmed. Electric door locks on emergency exits should revert to a disabled state if power outages occur to enable safe evacuation. While this may be considered a security issue, personnel safety always takes precedence, and these doors should be manned in an emergency.
- **Media Protection:** Location of media libraries, fire proof cabinets, kind of media used (fungi resistant, heat resistant).
- **Sprinkler system and fire resistance:** The fire-resistance rating of construction material is a major factor in determining the fire safety of a computer operations room. Generally, the computer room must be separated from other occupancy areas by constructional with a fire-resistant rating of not less than two hours.
- **Water or gas lines:** Water drains should be “positive;” that is, they should flow outward, away from the building, so they do not carry contaminants into the facility.

- **Air conditioning:** AC units should have dedicated power circuits. Similar to water drains, the AC system should provide outward, positive air pressure and have protected intake vents to prevent air carried toxins from entering the facility.
- **Electrical requirements:** The facility should have established backup and alternate power sources.

ii. Facilities Planning

As part of facilities planning, the security policy should provide for specific procedures for analysis and approval of facilities building and refurbishment plan. Depending on the size and nature of computing facilities, a separate function should exist for facilities planning and management. The following aspects need to be considered in this context:

- As part of environmental security clearance, procedures should be prescribed to ensure that all aspects relating to facilities planning are adequately considered.
- Approved list of materials to be used for construction of facilities, based on the class of computing facilities, the specification of equipment to be housed in such facilities should need consideration.
- The organisation chart should provide for designated personnel assigned with the responsibility of risk assessment procedures as a dynamic function.
- The risk profile of the organisation should take into consideration newer environmental threats. A few examples of threats to be considered are given below:
- Installation of a generator by a neighbour.
- Sudden changes in climate leading to extreme changes in humidity levels.
- Building construction in the vicinity of IPF leading to increase in suspended dust particles in the environment.
- Raising of foundation and flooring by a neighbour causing change in the flow of rainwater.
- Installation of high power consumption equipment adversely affecting the quality of power.

iii. Documentation

The documentation of physical and geographical location and arrangement of computing facilities and environmental security procedures should be modified promptly for any changes thereto. Access to such documentation should be strictly controlled. For example, knowledge of location and scheme of ventilation ducts can be used by a perpetrator to gain unauthorised entry to sensitive facilities which otherwise may be secured by physical and logical controls.

iv. People Responsibility and Training

Responsibility and accountability for environmental controls planning and management should be fixed and should be expressly communicated as part of job description. Awareness and training initiatives should encompass educating employees and stakeholders on environmental exposures and controls and their responsibilities thereof. New employee induction programmes should include informing and educating employees on environmental control procedures, prohibited activities (eating, smoking, drinking inside IPF), and maintaining secrecy and confidentiality. Care should also be taken to ensure that sharing such information should not result in risks, where unauthorised persons could gain knowledge of sensitive environmental control vulnerabilities.

v. Emergency Plan

Disasters result in increased environmental threats e.g. smoke from a fire in the neighbourhood or in some other facility of the organisation would require appropriate control action, evacuation plan should be in place and evacuation paths should be prominently displayed at strategic places in the organisation.

- *Reporting procedures* should be in place to enable and support reporting of any environmental threats to a specified controlling authority.
- *Periodic inspection, testing and supervision* of environmental controls should form a part of the administrative procedures. The tests of such inspection, tests and drills should be escalated to appropriate levels in the organisation.
- *Documented and tested emergency evacuation plans* should consider the physical outlay of the premises and orderly evacuation of people, shut down of power and computer equipment, activation of fire suppression systems.
- *Administrative procedures* should also provide for Incident Handling procedures and protocols due to environmental exposures.

vi. Vendors/Suppliers (Third Party)

In most cases installation and maintenance of environmental controls involves the services of third parties such as air conditioning, fire safety equipment, civil contractors, and carpenters. By virtue of their scope of work, knowledge of and access to sensitive computing facilities and environmental control vulnerabilities are available to such agencies. Procedures should include detailed analysis of considerations such as, whether to outsource, choice of such agency, background verification, security bonding, controlled access of maintenance staff and performance appraisal.

vii. Maintenance Plans

A comprehensive maintenance and inspection plan is critical to the success of environmental security and controls. Preventive maintenance plan and management procedures should be in place. This is a critical aspect of environmental control procedures, negligence in respect of which can lead to exposing the IPF to risks, e.g. prolonged ineffectiveness/failure of air conditioning facility can lead to risks of damage to servers and thereby loss of organisational data; a fire extinguisher not working at time of disaster due to negligence in refilling and maintenance. Maintenance plans should also include evaluation of effectiveness and efficiency of environmental facilities such as electric power distribution, heating plants, water, sewage, and other utilities required for system operation or staff comfort. Environmental controls should be documented and a suitable preventive maintenance should be put in place administered through schedules and logs.

viii. MTBF and MTTR

Failure modes of each utility, risks of utility failure, should be identified, parameterised and documented. This includes estimating the MTBF (Mean Time Between Failures) and MTTR (Mean Time To Repair/recover/respond/ restore). Planning for Environmental controls would need to evaluate alternatives with low MTBF or installing redundant units. Stocking spare parts on site and training maintenance personnel can reduce MTTR. Each of these strategies can be evaluated by comparing the reduction in risk with the cost to achieve it.

ix. Fire-resistant walls, Floors and Ceilings

The construction of IPF should use fire-resistant materials for walls, floors and ceilings. Depending on application and investment, manufacturers offer materials with varied fire ratings. Fire rating resistance of at least 2 hours is generally recommended.

x. Concealed Protective Wiring

Power and Communication cables should be laid in separate fire resistant panels and ducts. The quality rating of power cables should match the load and manufacturers specifications.

xi. Ventilation and Air Conditioning

The temperature in the IPF should be controlled depending on the type of equipment and processing. Improper maintenance of temperature leads to overheating of internal components. It should be examined if uninterruptible powers supply systems should supply power HVAC equipment that supports critical IPF units.

xii. Power Supplies

Computing equipment can be subject to risks of power failure and other power anomalies. Power supply should conform to computing equipment manufacturer specifications. Many elements can threaten power systems, the most common being noise and voltage fluctuations. Noise in power systems refers to the presence of electrical radiation in the system that is unintentional and interferes with the transmission of clean power. There are several types of noise, the most common being electromagnetic interference (EMI) and radio frequency interference (RFI). Voltage fluctuations are classified as Sag (momentary low voltage), Brownout (prolonged low voltage), and Spike (momentary high voltage), Surge (prolonged high voltage) and Blackouts (complete loss of power).

Some of the controls to ensure uninterrupted delivery of clean power are:

a. **Uninterruptible Power Supply (UPS)/ Generator:** UPS usually consist of battery backup or kerosene powered generator that interfaces with the external power supplied to the equipment. On interruption in external power supply, the control is immediately switched to the battery back-up. Depending on the application, UPS are available with battery backup of a few minutes to a number of days. UPS can be on-line or off-line. UPS generally is a good solution in case of applications enabling their proper closure of processing and systems. In respect of continuous process equipment, UPS may fail to meet the purpose if regular power supply is not available for a prolonged period of time. Diesel or kerosene generators could also be used, but they require some time to be switched on and the power from generators has to be cleansed before delivery to computer systems.

b. **Electrical Surge Protectors/Line Conditioners:** Power supply from external sources such a grid and generators are subject to many quality problems such as spikes, surges, sag and brown outs, noise, etc. Surge protectors, spike busters and line conditioners are equipment which cleanses the incoming power supply of such quality problems and delivery clean power for the equipment.

c. **Power leads from two sub-stations:** Failure of continued power supply to some high consumption continuous processing could even result in concerns regarding public safety such as refineries, nuclear reactors and hospitals. Electric power lines may be exposed to many environmental and physical threats such as foods, fire, lightning, careless digging, etc. To protect against such exposures, redundant power lines from a different grid supply should be provided for. Interruption of one power supply should result in the system immediately switching over to the stand-by line.

xiii. Smoke Detectors and Fire Detectors

Smoke and fire detectors activate audible alarms or fire suppression systems on sensing a particular degree of smoke or fire. Such detectors should be placed at appropriate places, above and below the false ceiling, in ventilation and cabling ducts. In case of critical facilities, such devices must be linked to a monitoring station (such as fire station). Smoke detector should supplement and not replace fire suppression systems.

xiv. Fire Alarms

Manually activated fire alarms switches should be located at appropriate locations prominently visible and easily accessible in case of fire (but should not be easily capable of misuse during other times). By manual operation of switch or levers, these devices activate an audible alarm and may be linked to monitoring stations both within and/or outside the organisation.

xv. Emergency Power Off

When necessity of immediate power shutdown arises during situations such as computer facility fire or emergency evacuation, emergency power-off switches should be provided. There should be one within the computer facility and another just outside the computer facility. Such switches should be easily accessible should be shielded to prevent accidental use.

xvi. Water Detectors

Risks to IPF equipment from flooding and water logging can be controlled by use of water detectors placed under false flooring or near drain hole. Water detectors should be placed on all unattended or unmanned facilities. Water detectors on detecting water activate an audible alarm.

Centralized Disaster Monitoring and Control Systems: Such systems provide for an organisation-wide network control wherein all detection devices, alarms and corrective/suppression devices are controlled from a central monitoring command and control. It is necessary that such systems are powered by a more secure and reliable/uninterrupted power supply. Such systems should be failure tolerant and involve low maintenance

xvii. Fire Suppression Systems

Combustibles are rated as either Class A, B, or C based upon their material composition, thus determining which type of extinguishing system or agent is used. Fires caused by common combustibles (like wood, cloth, paper, rubber, most plastics) are classed as Class A and are suppressed by water or soda acid (or sodium bicarbonate). Fires caused by flammable liquids and gases are classed as Class B and are suppressed by Carbon Dioxide (CO), soda acid, or FM200. Electrical fires are classified as Class C fires and are suppressed by Carbon Dioxide (CO), or FM200. Fire caused by flammable chemicals and metals (such as magnesium and sodium) are classed as Class D and are suppressed by Dry Powder (a special smothering and coating agent). Class D fires usually occur only places like chemical laboratories and rarely in office environments. Note that using the wrong type of extinguisher while suppressing a fire can be life-threatening. Broadly, Fire Suppression systems for facilities are classed into

a. Water based systems and

b. Gas based systems

a. Water Based Systems

- **Wet Pipe Sprinklers:** In this case, sprinklers are provided for at various places in the ceiling or on the walls and water is charged in the pipes. As generally implemented a fusible link in the nozzle melts in the event of a heat rise, causing a valve to open and allowing water to flow. These are considered the most reliable but however they suffer from the disadvantage of leakage, breakage of pipes exposing the IPF to the risks of dampness and equipment suffering water damage.
- **Dry-Pipe Sprinklers:** These are similar to the wet pipe sprinklers except that in this the water is not kept charged in pipes but pipes remain dry and upon detection of heat rise by a sensor, water is pumped into the pipes. This overcomes the disadvantage with wet pipe systems of water leakages etc.
- **Pre-action:** At the present time, this is the most recommended water-based fire suppression system for a computer room. It combines both the dry and wet pipe systems by first releasing the water into the pipes when heat is detected (dry pipe) and then releasing the water flow when the link in the nozzle melts (wet pipe). This feature enables manual intervention before a full discharge of water on the equipment occurs.

b. Gas Based Systems

- **Carbon-dioxide:** Such systems discharge CO thus effectively cutting of oxygen supply from the air, which is a critical component for combustion. However, CO being potentially lethal for human life, such systems are recommended only in unmanned computer facilities or in portable or hand-held fire extinguishers. Portable fire extinguishers commonly contain CO or soda acid and should be commonly located at exits, clearly marked with their fire types Checked regularly by licensed personnel.

- **FM200:** Halon was once considered the most suitable agent for fire suppression. FM200 is an inert gas, does not damage equipment as water systems do and does not leave any liquid or solid residues, however it is not safe for humans as it reduces the levels of oxygen. Halon is not considered safe for environment as it is an ozone-depleting agent. Under an international agreement, the Montreal Protocol, the production of Halon has been suspended from 1994 and FM 200 replaced the Halon.

4.3.3 Integration and fine-tuning of environmental controls

As part of environmental risk assessment, facilities planning and facilities management, it is critical to consider the overall effectiveness, efficiency of controls. Planning for environmental controls should consider interdependencies of IS assets being secured, vulnerabilities of such assets and related nature of other controls such as logical and physical access controls. The security policy should orchestrate the overall design; effectiveness and efficiency of controls to ensure that investment in environmental controls are optimum without compromise on security.

4.3.4 Audit and evaluation of Environmental Controls

As part of audit procedures, the audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices, which may include the following activities:

- Inspect the IPF and examine the construction with regard to the type of materials used for construction by referring to the appropriate documentation.
- Visually examine the presence of water and smoke detectors, examine power supply arrangements to such devices, testing logs, etc.
- Examine location of fire extinguishers, fire-fighting equipment and refilling date of fire extinguishers and ensure their adequate and appropriate.
- Examine emergency procedures, evacuation plan and marking of fire exits. If considered necessary, the IS Auditor can also require a mock drill to test the preparedness with respect to disaster.
- Examine documents for compliance with legal and regulatory requirements as regards fire safety equipment, external inspection certificate, shortcomings pointed out by other inspectors/auditors.
- Examine power sources and conduct tests to assure quality of power, effectiveness of power conditioning equipment, generators, simulate power supply interruptions to test effectiveness of back-up power.
- Examine environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc.
- Examine complaint logs and maintenance logs to assess if MTBF and MTTR are within acceptable levels.
- Observe activities in the IPF for any undesired activities such as smoking, consumption of eatables etc.

Documentation of findings

As part of the audit procedures, the IS auditor should document all findings as part of working papers. The working papers could include audit assessment, audit plan, audit procedure, questionnaires, and interview sheets, inspection charts, etc.

Examples of environmental controls and their Audit procedures

Control Activities	Control Techniques	Audit Procedures
Safeguards against the risks of heating, ventilation and air-conditioning systems.	Identify systems that provide constant temperature and humidity levels within the organisation.	Review a heating, ventilation and air-conditioning design to verify proper functioning within an organisation.
Control of radio emissions effect on computer systems.	Evaluate electronic shielding to control radio emissions that affect the computer systems.	Review any shielding strategies against interference or unauthorised access through emissions.
Establish adequate interior security based on risk	Critical systems have emergency power supplies for alarm systems; monitoring devices, exit lighting, communication systems.	Verify critical systems (alarm systems, monitoring devices, and entry control systems) have emergency power supplies. Identify back -up systems and procedures and determine the frequency of testing. Review testing results.
Adequately protect against emerging threats, based on risk.	Appropriate plans and controls such as shelter in place or for a potential CBR attack(chemical, biological and radioactive attack) Restricting public access and protect critical entry points-air intake vents, protective grills and roofs.	Interview officials, review planning documents and related test results. Observe and document the controls in place to mitigate emerging threats. Observe location of these devices and identify security measures implemented. Verify the controls existence and intrusion detection sensors.
Adequate environmental controls have been implemented	Fire detection and suppression devices are installed and working.(smoke detectors, fire extinguishers and sprinkle systems)	Interview managers and scrutinize that operations staff are aware of the locations of fire alarms, extinguishers, shut-off power switches, air -ventilation apparatus and other emergency devices.

Control Activities	Control Techniques	Audit Procedures
	Controls are implemented to mitigate disasters, such as floods, earthquakes.	Determine that humidity, temperature and voltage are controlled within the accepted levels.
	Redundancy exists in critical systems like, uninterrupted power supply, air cooling system, and backup generators Humidity, temperature, and voltage control are maintained and acceptable levels	Check cabling, plumbing, room ceiling smoke detectors, water detectors on the floor are installed and in proper working order.
	Emergency lighting, power outages and evacuation routes are appropriately located.	
Staff have been trained to react to emergencies	Operational and support personnel are trained and understand emergency procedures. Emergency procedures are documented and periodically tested- incident plan, inspection plan and maintenance plan.	Interview security personnel to ensure their awareness and responsibilities. Review training records and documentation. Determine the scope and adequacy of training. Review test policies, documentation and know-how of operational staff. Review incident handling procedures and maintenance and inspection plan.

4.4 Summary

This chapter deals with the physical and environmental threats and their control and audit procedures on information system assets. The first step in providing a secured physical environment for the information system assets is listing the various assets in the computing environment. These assets could range from hardware, software, facilities and people that form the computing environment. The next step is to identify the various threats and exposures the assets are exposed to. These threats could include unauthorised access to the resources, vandalism, public disclosure of confidential information and the like, the main source of threats is from outside people and the employees of the organisation. However, the information assets are exposed to various other sources of threats like natural damage due to environmental factors like food, earthquake, fire and rain etc.

4.5 Questions

1. Which of the following is first action when a fire detection system raises the alarm?
   - A. Turn off the air conditioning
   - B. Determine type of fire
   - C. Evacuate the facility
   - D. Turn off power supply
2. Which of the following is most important controls for unmanned data center?
   - A. Access control for entry and exit for all doors
   - B. The humidity levels need not be maintained
   - C. The temperature must be at sub-zero level
   - D. Halon gas based fire suppression system
3. Primary purpose of access controlled deadman door, turnstile, mantrap is to:
   - A. Prevent unauthorised entry
   - B. Detect perpetrators
   - C. Meet compliance requirement
   - D. Reduce cost of guard
4. Which of the following is main reason for appointing human guards at main entrance of facilities?
   - A. Address visitors' requirements to visit
   - B. Issue the access cards to visitors
   - C. Cost of automation exceeds security budget
   - D. Deter the unauthorised persons
5. Which of the following is major concern associated with biometric physical access control?
   - A. High acceptability
   - B. High false positives
   - C. High false negatives
   - D. High cost
6. Which of the following evidence is best to provide assurance on automated environmental controls?
   - A. Annual maintenance contract with vendor
   - B. Simulation testing of devices during audit
   - C. Device implementation report by vendor
   - D. Documented results of periodic testing

7. What are the problems that may be caused by humidity in an area with electrical devices?
   - A. High humidity causes excess electricity, and low humidity causes corrosion.
   - B. High humidity causes power fluctuations, and low humidity causes static electricity
   - C. High humidity causes corrosion, and low humidity causes static electricity
   - D. High humidity causes corrosion, and low humidity causes power fluctuations

8. Automated access controls opens doors based on access cards, pins, and/or biometric devices and are powered by electricity. Which of the following best policy in case of power failure?
   - A. Keep the door in locked state
   - B. Open door and appoint guard
   - C. Find root cause of power failure
   - D. Arrange for battery backup

9. While selecting site for a data centre which of the site is best to be selected?
   - A. On topmost floor to delay the unauthorised visitor to reach
   - B. In the basement not easily accessible to perpetrator
   - C. On ground floor do that users can access is easily
   - D. On middle floor to strike the balance for above concerns

10. Which of the following is main reason for not allowing mobile devices into data centre?
    - A. Unauthorised changes and access in configuration
    - B. Prevent photography of data centre layout
    - C. User can provide information to attacker on phone
    - D. Mobile devices generate wireless communication

4.6 Answers and Explanations

1. C. Life safety takes precedence. Although other answers are important steps human life always is a priority.
2. A. Unmanned data centre requires strong physical access controls and environmental access controls too. However most essential are strong access controls. B, C and D are inappropriate controls. Halon is environmentally hazardous gas.
3. A. Primary purpose of all types of physical access control is to prevent unauthorised entry. Other objectives are secondary.
4. A. Human guard make decisions and can address visitor's requirement and direct them appropriately. Others are supplementary functions.
5. B. False positive is a concern in biometric access security as it results in unauthorised access. Other option does not result in unauthorised access.

6. D. Automated environmental controls must be tested periodically by expert and provide report on effective performance of equipment. Simulated tests may not be possible for all controls. AMC is a contract, periodic testing is performance of contract.

7. C. High humidity can cause corrosion, and low humidity can cause excessive static electricity. Static electricity can short out devices or cause loss of information.

8. B. Best policy is to keep door open and appoint guard temporarily for monitoring accesses. Keeping doors locked shall be a problem in evacuation in case of emergency. Finding root cause can be done independently. Arranging Battery backup after power failure is not right policy.

9. D. Top floor and basement has risk of seepage and flooding. Ground floor has risk of easy attack.

10. A. Mobile devices can be connected to servers and resulting in unauthorised changes. Other concerns are secondary.

CHAPTER 5: LOGICAL ACCESS CONTROLS

5.1 Introduction

Virtually every day another news story highlights the importance of network security–corporate networks are breached, databases are accessed by unauthorised individuals, and identities are stolen and used to conduct fraudulent transactions. As a result, both businesses and governments are evaluating or implementing new identity management systems to provide more secure logical access. Today IT systems store and process a wide variety of data centrally in one system and provide access to the same to a large number of users. Keeping data stored centrally on a system contributes to cost effective and efficient information sharing and processing. In such an environment it is not unusual that there is a requirement that:

- Some information must be accessible to all users,
- Some is needed by several groups or departments,
- And some accessible by only a few individuals

Information that is residing on a system and accessed by many users has an associated risk of unauthorised access. Logical access controls are a means of addressing concerns associated with unauthorised accesses. Logical access controls are protection mechanisms that limit users' access to data and restrict their access on the system based on "need to know and need to do" basis. These access controls need to be part of assets that are designed to store and process information, i.e. application systems, database management systems, operating systems, middleware. However to minimise complexity organisations may choose to implement external access control systems like single sign-on, Citrix farm, LDAP and active directory etc. In this chapter, we will understand various ways that data can be accessed and how logical access controls can help to ensure that only the right persons access the right data.

5.2 Objectives of Logical Access Controls

The purpose of logical access controls is to prevent and detect unauthorised access to information assets/resources while ensuring that authorised users can access the information resources as per their role and responsibilities. This is achieved by providing access on "need to know and need to do" basis using principle of least privileges. It means that the access should not be so restrictive that it makes the performance of business functions difficult or it should not be so liberal that it can be misused i.e. it should be just sufficient for one to perform one's duty without any problem or restraint. Logical access controls is all about protection of information assets in all three states, namely: stored, in transit and being processed

5.3 Paths of Logical Access

An auditor has to identify the possible access paths permitting access to information resources. Auditor must document the logical paths and prescribe appropriate audit procedures to evaluate every component in the information systems infrastructure to enable identification of logical access paths. This is often a challenging and complex task when it comes to auditing in networking computing environments. Identification and documentation of access paths involves testing security at various layers:

- **Hardware:** This includes computer workstations, terminal devices, communication devices, peripherals etc., constituting the physical interface with the users. Here the auditor should consider vulnerabilities of different communication channels and devices (e.g. modems, network interface cards) connected to computers.
- **Systems software:** The command and control of hardware rests in the proper implementation of operating systems and other systems software. Hardware works in tandem with, and its operation is synchronised by, systems software which forms the foundation for effective systems security. From a logical perspective, a wrong setting of systems level parameters can compromise the security of the application and other systems software, which talk to the systems software. Auditor should ensure that logical accesses to system software are controlled to prevent and/or detect changes in system configuration.
- **Database Management System:** In environments involving voluminous data handling, a Database Management System (DBMS) manages the organisation of data in the databases. The auditor is required to evaluate the access security enforced by the DBMS, which could include schema definitions, access to data dictionary, directory services and scripts to restrict access implemented by the DBMS.
- **Application software:** Application software represents the business logic, which interfaces with the user and business process requirement, from the user perspective. The auditor focuses on the effectiveness of boundary controls and other input, processing and output controls, discussed elsewhere in this module.
- **Access control software:** The auditor may also encounter situations in networked environments with users having access to various applications. In such cases user and programme access to applications and IS resources are controlled by an access control software. The auditor should evaluate the access permissions configured in the software and ascertain their appropriateness to the organisation's functional requirements.
- In the above cases, the assessment of state of access controls can be quite technical, presenting complexities for the IS auditor. Therefore, in cases, where the controls involve technical sophistication, the auditor has to rely on the services of a technical expert, who possesses special skills, knowledge and experience in the particular field. Where the auditor relies on the work of an expert, he should evaluate the work and the extent of reliance on the work of the expert. The auditor's report should explicitly state this fact of IS auditor's reliance on work of other experts.

Each of these routes has to be subjected to appropriate means of security in order to secure it from the possible logical access exposures.

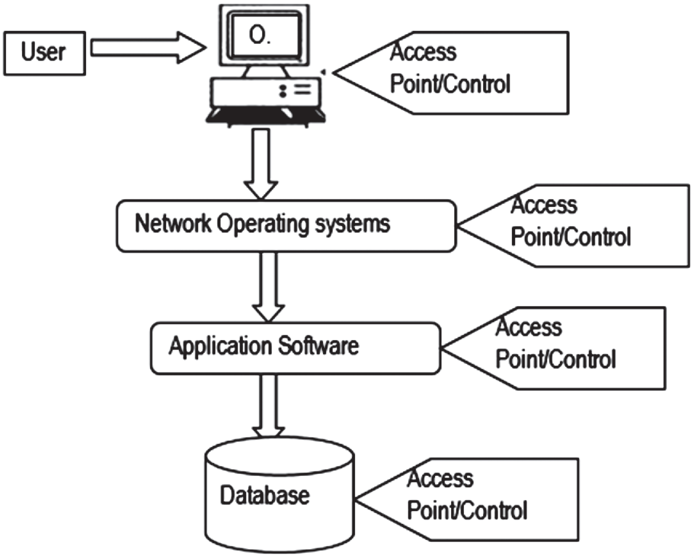


Figure 5.1: Logical Access Paths in an Enterprise Information System

5.4 Logical Access attacks

Improper logical access can result in loss or damage to information and resources leading to undesirable consequences for an organisation. It can also result in violation of the confidentiality or integrity or availability of information. There are various types of exposures related to access controls where unauthorized persons tried to get information useful for breaking into organisation system. These attacks can be grouped based on the object of attack i.e. Technology and/or user. Some of the technical attacks are discussed below:

Masquerading: It means disguising or impersonation. The attacker pretends to be an authorised user of a system in order to gain access to or to gain greater privileges than they are authorised for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programmes, or through bypassing the authentication mechanism. The attempt may come from within an organisation, for example, from an employee; or from an outside user through some connection to the public network. Weak authentication provides one of the easiest points of entry for a masquerade. Once the attacker has been authorised for entry, they may have full access to the organisation's critical data, and (depending on the privilege level they pretend to have) may be able to modify and delete software and data or make changes.

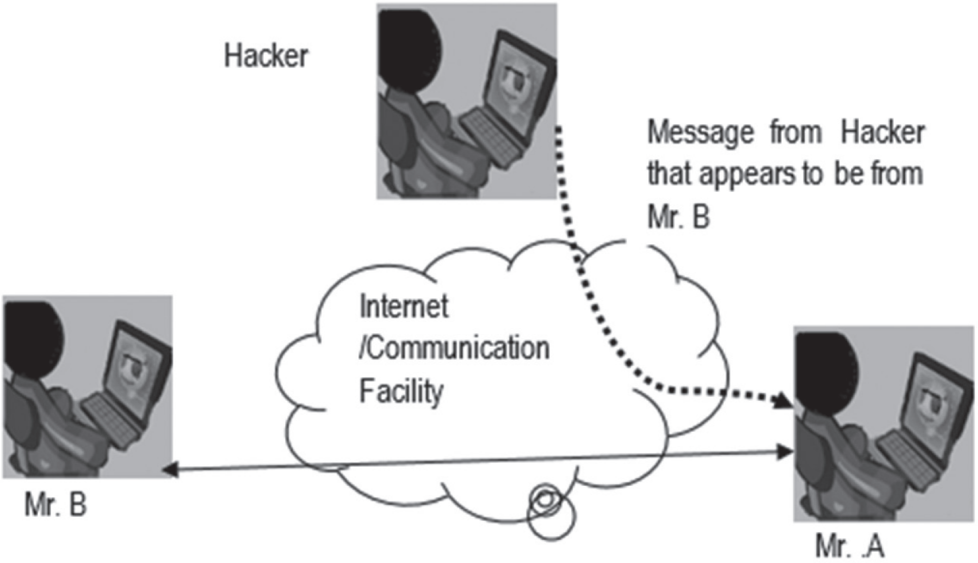

Hacker
Message from Hacker that appears to be from Mr. B
Internet /Communication Facility
Mr. B
Mr. .A

Figure 5.2: Masquerade or impersonating

Piggybacking: Unauthorized access to information by using a terminal that is already logged on with an authorized ID (identification) and left unattended.

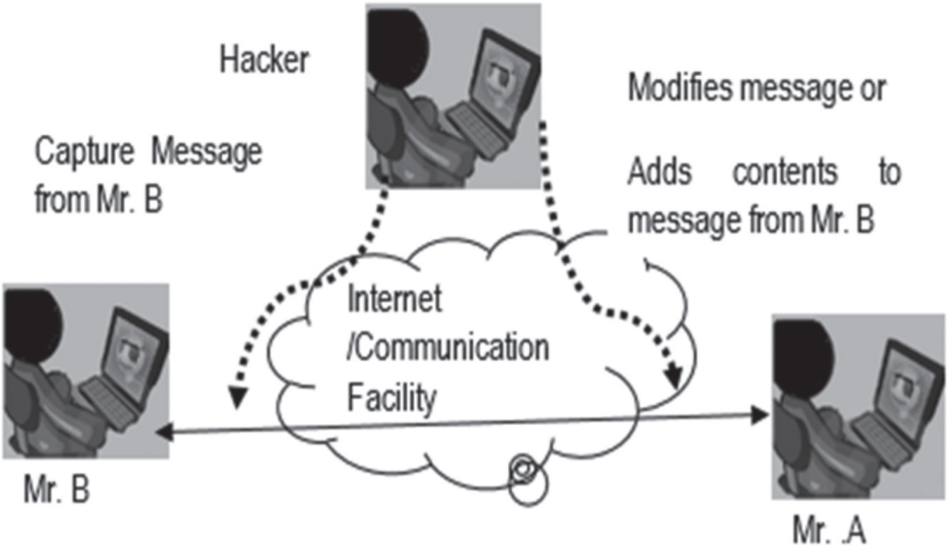

Hacker
Capture Message from Mr. B
Modifies message or
Adds contents to message from Mr. B
Internet /Communication Facility
Mr. B
Mr. .A

Figure 5.3: Piggybacking i.e. following authorised user

Wiretapping: Tapping a communication cable to collect information being transmitted.

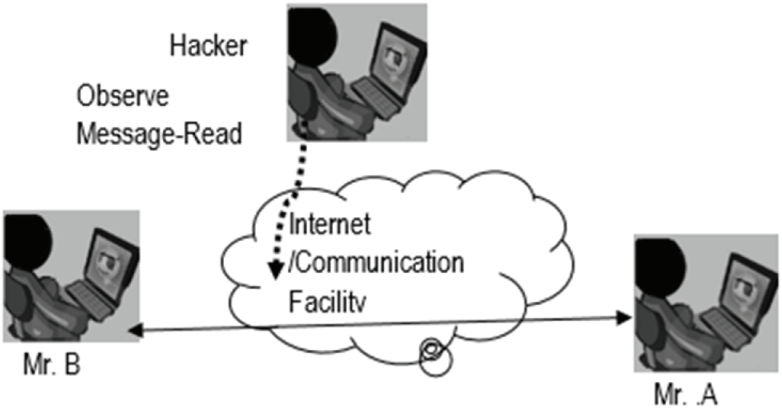


Figure 5.4: Wiretapping a passive attack to collect information

Denial of Service: The perpetrator attempts to flood memory buffers and communication ports to prevent delivery of normal services. (Covered in next chapter)

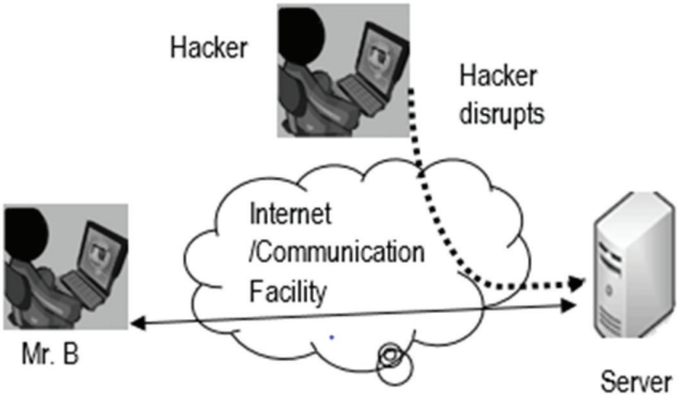


Figure 5.5: Denial of Service by disrupting traffic

5.4.1 Social Engineering

This is an attack on the weakest link i.e. human. The perpetrators uses different means including spoofing and masquerading resulting in person reveals confidential information like user ID, Password, PIN and any such information required for login as authorised user.

Examples of some of these attacks are:

- **Phishing:** User receives a mail requesting to provide authentication information by clicking on link provided. The mail and link appears to be actual originator e.g. Bank. Unaware users click on link and provide confidential information. The most popular attacks on banking systems in the recent times, they target gullible victims, using a combination of social engineering, e-mail and fake websites to con the victim to click on a link embedded in an apparent authentic mail from a reputed bank. The link takes the victim (generally a customer of the bank) to a look-alike Bank website that gets the personal details of the victim including details such as PIN and internet banking password, which is then exploited by the hacker.

- **Impersonating:** Uses the similar technique over telephone.
- **Key logger:** Perpetrator installs software that captures the key sequence used by user including login information. Key logger can be sent thru mail or infected pen drive like virus or other malware. There are hardware key loggers available that are connected to system where key board is attached.
- **Malware:** Specially designed programmes that captures and transmits the information from compromised system.
- Malicious code (also called "Malware") is the name used for any programme that adds to, deletes or modifies legitimate software for the purpose of intentionally causing disruption and harm or to circumvent or subvert the existing system's function. Examples of malicious code include viruses, worms, Trojan Horses, and logic bombs. Newer malicious code is based on Active X and Java applets.

Viruses:	• Are malicious code that attaches to a host programme and propagates when an infected programme is executed? The perpetrator's objective is to multiply and spread the code. However they are dependent on another programme or human action to replicate or to activate their payload. They are not capable of self-actuating.
Worms:	• Are malicious programmes that attack a network by moving from device to device and create undesirable traffic. • They differ from viruses in that for replication or activation of code, they do not depend on any programmes or human action but are self-actuating and self-sustaining and spread much more rapidly than viruses.
Trojan Horses:	• These are malicious code which hides inside a host programme that does something useful. Once these programmes are executed, the hidden malicious code is released to attack the workstation, server, or network or to allow unauthorised access to those devices. Some Trojans are programmed to open specific ports to allow access for exploitation. Then the open Trojan port could be scanned and located, enabling an attacker to compromise the system. These are also used as tools to create backdoors into the network for later exploitation by crackers.
Logic Bombs:	• These are legitimate programmes, to which malicious code has been added. Their destructive action is programmed to "blow up" on occurrence of a logical event such as time or a logical event as number of users, memory/disk space usage, etc.

	• Every time the infected programme is run, the logic bomb checks external environment to see whether the condition to trigger the bomb has been met. If not, control is passed back to the main application and the logic bomb waits. If the condition is satisfied, the rest of the logic bomb's code is executed, and it attacks the system. • Logic bombs are very difficult to detect since they reside in the system and its destructive instruction set is known only after it blows up.
Macro Viruses:	• A macro is an instruction that carries out programme commands automatically. Many common applications (e.g. word processing, spreadsheet, and slide presentation applications) make use of macros. • A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or an event trigger. If a user accesses a document containing a viral macro and unwittingly executes this macro virus, it can then copy itself into that application's start-up files. • The computer is now infected and a copy of the macro virus resides on the machine. Any document on the machine that uses the same application can become infected. If the infected computer is on a network, the infection is likely to spread rapidly to other machines on the network. Because these types of files are commonly used and sent through e-mail, a computer network can be quickly infected by these viruses. • Macro viruses tend to be surprising but relatively harmless.
Polymorphic Viruses	• Polymorphic viruses are difficult to detect because they hide themselves from antivirus software by altering their appearance after each infection. Some polymorphic viruses can assume over two billion different identities.
Stealth Viruses	• Stealth viruses attempt to hide their presence from both the operating system and the antivirus software by encrypting themselves. They are similar to polymorphic viruses and are very hard to detect.
Adware and Spyware	• They are often software that tracks the Internet activities of the user usually for the purpose of sending targeted advertisements. • Besides the loss of privacy and waste of bandwidth (loss of availability), they do not pose other security related risks, as yet. However, it is quite likely that Trojans could be embedded in such software. • Adware and Spyware often come with some commercial software, both packaged as well as shareware software. There is often a reference to the Adware and Spyware software in the licence agreement.

5.5 Logical Access Controls Policy and Procedures

Access control policy is part of overall information Security policy It states a set of rules, principles, and practices that determine how access controls are to be implemented access control policy typically covers the following:

- User management
- User responsibilities
- Network access controls
- Application access controls
- Database access controls
- Operating system access controls

5.5.1 User management

It is a process to manage access privileges for identified and authorised users. The steps involved are:

- User registration
- Privilege management
- Password management
- Review and monitoring accesses
- Revocation of access privilege.

User registration

It refers to identifying a user who needs to access information asset. This is generally done based on the job responsibilities and confirmed by User manager. This must be approved by information owner. User registration process must answer:

- Why the user is granted the access?
- Has the data owner approved the access?
- Has the user accepted the responsibility?

Privilege management

Access privileges are to be aligned with job requirements and responsibilities. These are defined and approved by the information asset owner. For example, an operator at the order counter shall have direct access to order processing activity of the application system or an assistant in Bank may have access to enter transaction and a manager can only approve but cannot enter the transaction. Changes in privileges are common activity based on changes in roles of users. Sometimes some users are provided additional privileges for temporary period or during emergencies. Revoking them need to be part of process. Many a times application or database privilege management does not provide for automatic revocation of such accesses. In these cases manual monitoring and periodic reviews are compensating controls to correct the situation.

Password management

Password management is controlled based on the password policy. Passwords are used to authenticate user for access to systems. Password management functions include:

- Allocations of password which is generally done by system administrators
- Secure communication of password to appropriate user
- Force change on first login by the user so as to prevent possible misuse by system administrators
- Storage of password is generally should not be done in plain text. Most system stores password as hash of actual password.
- Authentication process is verifying password and user ID provided by user. Passwords are verified by generating hash and then hash is compared with stored hash.
- Password expiry must be managed as per policy. Users must change passwords periodically and system should be configured to expire the password after predefined period. Password may also be expired after predefined limit of unsuccessful logins.
- Reissue of password after confirming the identity of users in case of expired password or if users have forgotten the passwords. This process is typically same as allocation of password.
- Educating users is a critical component about passwords, and making them responsible for their password.

Review of user access rights

Periodic review of user's access rights is essential process to detect possible excess rights due to changes in responsibilities, emergencies, and other changes. These reviews must be conducted by information owner and administrators facilitates by providing available accesses recorded in system.

Default Users

Applications, operating systems and databases purchased from vendor have provision for default users with administrative privileges required for implementation and/or maintenance of application, OS or database. The user ID and Passwords for these users are published by the vendor required for implementing. It is expected that these password must be changed immediately as soon as system is implemented. While reviewing these access controls IS auditor must ensure that these user ID are either disabled, or passwords have been changed and suitably controlled by the organisation.

5.5.2 User responsibilities primarily include:

- User awareness about responsibility associated with access privileges granted
- Password change and use, particularly ensuring they are not shred intentionally or accidentally

  Mandatory use of strong passwords to maintain confidentiality.

- Users should ensure that none of the equipment under their responsibility is ever left unprotected.
- Users should also secure their PCs with a password, and should not leave it accessible to others.

5.5.3 Network access control

Network access controls refers to the process of managing access for use of network based services like shared resources, access to cloud based services, remote login, network and internet access. There are various tools and techniques used to manage these accesses. Network based tools and techniques like protocol control, service monitoring are discussed in network security chapter.

Policy on use of network services

An enterprise wide applicable internet service requirements aligned with the business need policy based on business needs for using the Internet services is the first step. Selection of appropriate services and approval to access them will be part of this policy. The policy also specify the use on internet and internet based services while access internet using organisation's devices.

Segregation of networks

Based on the sensitive information handling function; say a VPN connection between a branch office and the head-office this network is to be isolated from the internet usage service availability for employees.

Network connection and routing control

The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility. The techniques of authentication and authorisation as per access policy have been implemented across the organisation's network.

Enforced path

Based on risk assessment, it is necessary to specify the exact path or route connecting the networks; say for example internet access by employees will be routed through a firewall. And to maintain a hierarchical access levels for both internal and external user logging. An Internet connection exposes an organisation to the entire world. This brings up the issue of benefits the organisation should derive along with the precaution against harmful elements.

Clock synchronisation

Clock synchronization is useful control to ensure that event and audit logs maintained across an enterprise are in synch and can be correlated. This helps in auditing and tracking of transactions along with date and time that is uniform across organisation. In modern networks this function is centralised and automated.

5.5.4 Application and monitoring system access control

Applications are most common assets that accesses information. Users invoke the programmes/ modules of application to access, process and communicate information. Hence it is necessary to control the accesses to application. Most modern applications provide independent user and access privilege management mechanism for example ERP, Core Banking applications. However, legally or old application may rely in database management system or operating system used to host these applications. In case of legacy applications IS auditors may have to review accesses at all layers i.e. application, database and/or operating systems. Ideally database administrators and system administrators are only roles that need to have access to database and operating system respectively.

The access to information is prevented by application specific menu interfaces, which limit access to system function. A user is allowed to access only to those items he is authorised to access. Controls are implemented on the access rights of users, For example, read, write, delete, and execute. And ensure that sensitive output is sent only to authorised terminals and locations.

Sensitive system isolation

Based on the critical constitution of a system in an enterprise it may even be necessary to run the system in an isolated environment. Monitoring system access and use is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect and report any unauthorised activities.

Event logging

In Computer systems it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly.

Monitor system use

Based on the risk assessment a constant monitoring of some critical systems is essential. Define the details of types of accesses, operations, events and alerts that will be monitored. The extent of detail and the frequency of the review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs.

5.5.5 Database access controls

Database management systems like oracle provide user management mechanism. DBA can build profile with settings defined by security policies. These profiles are then assigned to roles defines to performs functions on database like view, update, delete, commit. These roles are then assigned to users created on database. Generally these are stored in user table. Databases also provide storing of password hash for each user thus DBA can access but may not find out the password of users. Application developed to use this database can use database login mechanism for providing access to users. (More information on DB access control is provided in section 5.16.

5.5.6 Operating system access control

Operating system provides the platform for an application to use various IS resources and perform the specific business function. If an intruder is able to bypass the network perimeter security controls, the operating system is the last barrier to be conquered for unlimited access to all the resources. Hence, protecting operating system access is extremely crucial. Some of the key controls of operating system are outlined here.

- **Automated terminal identification:** This will help to ensure that a particular session could only be initiated from a particular location or computer terminal.
- **Terminal log-on procedures:** The log-on procedure does not provide unnecessary help or information, which could be misused by an intruder.
- **User identification and authentication:** The users must be identified and authenticated in a fool proof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.
- **Password management system:** An operating system could enforce selection of good passwords. Internal storage of password should use one-way encryption algorithms and the password file should not be accessible to users.
- **Use of system utilities:** System utilities are the programmes that help to manage critical functions of the operating system-for example, addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.
- **Duress alarm to safeguard users:** If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities. An example could be forcing a person to withdraw money from the ATM. Many banks provide a secret code to alert the bank about such transactions.
- **Terminal/Session time out:** Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.
- **Limitation of connection time:** Define the available time slot. Do not allow any transaction beyond this time period. For example, no computer access after 8.00 p.m. and before 8.00 a.m. or on a Saturday or Sunday. This is useful in preventing unauthorised accesses by authorised users.

5.6 Audit Trail

Primary objective of access controls is fix the accountability to individual user for the activities performed by them. This can be done only by generating and reviewing activity logs. However many times IT persons are reluctant to generate log since logs are resource consuming. It requires additional storage, separate access controls, and programming efforts. The issue can be resolved by defining priorities based on risk assessment results and logs for select critical activities like system administration, changes in configuration, access to sensitive information, business transactions, may be enabled.

Logs are also called ‘audit trail’. It is a record of system activities that enables the reconstruction and examination of the sequence of events of a transaction, from its inception to output of final results. Violation reports present significant, security-oriented events that may indicate either actual or attempted policy transgressions reflected in the audit trail. Violation reports should be frequently and regularly reviewed by information owner to identify any unauthorised change or access.

Audit information comprises a history of transactions, including who processed the transaction, the date and time of the transition, where the transaction occurred, and related activities. An audit associated with information system security searches for the following:

- Internal and external attempts to gain unauthorised access to a system
- Patterns and history of accesses
- Unauthorised privileges granted to users
- Occurrences of intrusions and their resulting consequences

Depending upon requirements logs are generated at various levels. At application level logs of business transaction with time stamp are generated. These are used by auditors to perform audit. Administrator activity logs at application level, data base level, network device level and operating system level are critical to ensure security. Because of their importance, audit logs should be protected at the highest level of security in the information system.

5.7 Access controls and mobile computing

In today's organisations computing facility is not restricted to a particular data centre alone. Ease of access on the move provides efficiency and results in additional responsibility on users and the need to maintain information security on the management. Theft of data carried on the disk drives of portable computers is a high risk factor. Both physical and logical access to these systems is critical. Information is to be encrypted and access identifications like fingerprint, eye-iris, and smart cards are necessary security features.

5.8 Access control mechanism

Identification and Authentication The primary function of access control is to allow authorised access and prevent unauthorised access. Access control mechanism is actually a three step process as depicted in the figure below:

(a) **Identification:** Identification is a process by which a user provides a claimed identity to the system such as an account number.

(b) **Authentication:** Authentication is a mechanism through which the user's claim is verified.

(c) **Authorization:** The authenticated user is allowed to perform a pre-determined set of actions on eligible resources.

The primary function of access control is to allow authorised access and prevent unauthorised access to information resources in an organisation, therefore, it may become necessary to apply access control at each security architectural layer of an organisation's information system architecture to control and monitor access in and around the controlled area. This includes operating system, network, database and application systems. In each of these layers attributes may include some form of identification; authentication and authorisation and logging and reporting of user activities. Interfaces exist between operating system access control software and other system software access control programmes such as those of routers, firewalls etc. that manage and control access from outside or within organisation networks. On the other side operating system access control software may interface with databases and / or application system access controls to application data.Please see details in figure 5.6 in next page.

5.8.1 Identification Techniques

Of the above, implementing the right authentication is the most challenging. Authentication is the process of verifying that the identity claimed by the user is actually true. Users are authenticated using one of three personal authentication factors or techniques. The three categories of authentication factors are **Please see details in Figure 5.7 in following page**

- Something the user knows (e.g., a password),
- Something the user has (e.g., a token or smart card), and
- Something the user is (a physical / biometric comparison).

Single-factor authentication uses any one of these authentication factors. Two-factor or dual factor authentication uses two factors and the three-factor authentication uses all the three factors. Individual authentication assurance increases when multiple authentication technologies and techniques are combined and used. Authorized access to an information resource requires identification and authentication of the person requesting access.

Once the user is authenticated, the system must be configured to validate that the user is authorized (has a valid need-to-know) for the resource being protected and can be held accountable for any actions taken. Authorized access to logical assets can be implemented as a combination of manual, automated, and/or administrative methods. A deny-by-default policy, where access to the information resource is denied unless explicitly permitted should be mandated. The decision to grant or deny access to an information resource is the responsibility of the resource owner.

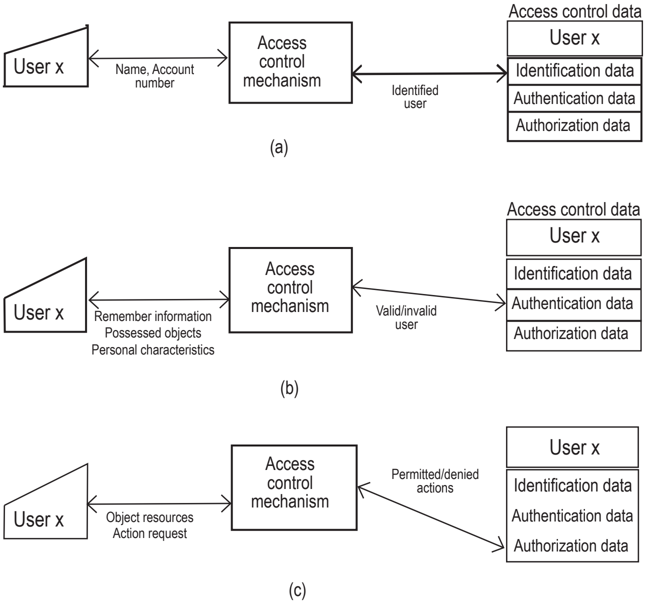


Figure 5.6: Identification, Authentication and Authorisation

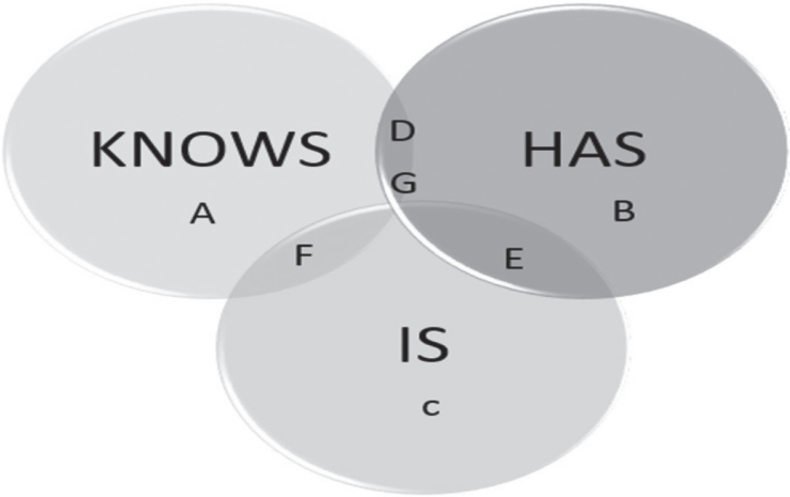


Figure 5.7: Multi-factor authentication.

A. Password

B. Identified Badge

C. Fingerprint

D. Bank Card and PIN

E. Smart Card with Biometric template

F. Fingerprint Detectors with PIN entry

G. Identifying Badge with Photograph and associated Password.

5.8.2 Authentication techniques

As stated above, authentication may be through remembered information, possessed tokens, or physical characteristics. We shall examine each class of authentication techniques below.

Figure 5.8: What you have (Token), what you know (password/PIN) and who you are (Biometric)

- **Passwords:** This is the most common authentication technique that depends on remembered information. The user, initially, identifies him using his login-id to the system and then provides the password information. Once the system is able to locate the match and is successful for both fields, the system authenticates the user and enables access to resources based on the authorization matrix. However if a match is not successful, the system returns a message (such as "Invalid User or password") thus preventing access to resources.
- **Personal Identification Numbers (PINs):** Is a type of password, usually a 4-digit numeric value that is used in certain systems to gain access, and authenticate. The PIN should be such that a person or a computer cannot guess it in sufficient time by using a guess and check method, i.e. where it guesses the PIN, and checks for correctness by testing it on the system that the person is attempting to gain access to and the process is repeated with a different guess till access is obtained. PINs are commonly used for gaining access to Automatic Teller Machines (ATMs).

One-Time Passwords

One-time passwords solve the problems of user-derived passwords. With one-time passwords, each time the user tries to log on he is given a new password. Even if an attacker intercepts the password, he will not be able to use it to gain access because it is good for only one session and predetermined limited time period. For example one time password for online card transaction is provided by bank to user on registered mobile is valid for 10 minutes only. One-time passwords typically use a small hardware device or software that generates a new password every time. The server also has the same software running, so when a user types in his password, the server can confirm whether it is the correct password. Each time the user logs on he has a new password, so it is much more secure.

Challenge Response

An alternative to one-time passwords is challenge response schemes. Instead of having the device just blindly generate a password, a user identifies himself to the server, usually by presenting his user ID. The server then responds with a challenge, which is usually a short phrase of letters and numbers. The user types the challenge into the device and, based on the challenge, the device responds with an output. The user then types that output in as his password to the server. This scheme is slightly more complicated, but it allows the password to be based on changing input rather than just time.

5.8.3 Weaknesses of Logon mechanism

Logon/password access security is based on information to be remembered by the user (what the user knows). This results in the following weaknesses:

- Passwords are easily shared
- Users often advertently or inadvertently reveal passwords leading to security being compromised
- Repeated use of the same password could lead to being easily guessed by others
- If a password is too short or too easy, the chances of it being guessed are quite high

- If a password is too long or too complex, the user may forget or may write it down
- If many applications are to be accessed by one user, many passwords have to be remembered
- Passwords can be shared, guessed, spoofed or captured

Recommended practices for strong passwords

- The user should not share the authentication information viz. password.
- The password should be easy for the user to remember but hard for the perpetrator to guess.
- On creation of a new user, the first password is allotted by the security administrator and a change of password is forced on the first login.
- Users should be encouraged or forced to change passwords periodically e.g. once in 60 days.
- Concurrent logins by same user should not be permitted.
- Passwords should not be too short and should not use name of user, pet-names, common words found in dictionary or such other attributes.
- Password combination should be random and use alphabetic, numeric and special characters (such as "!", "#", "^", etc.).
- Passwords should be changed periodically.
- Number of wrong login tries should be restricted to three, after which the system should lockout the user. Further access can be granted only through the intervention of the security administrator.
- The logon IDS active in the system should not exceed the number of users actually authorised to access systems resources.
- Passwords should be stored in an encrypted form using one-way encryption.
- In case the user remains inactive at a terminal, for a length of time (say 20 minutes), the terminal should lock out the user and require the user to login again.

5.8.4 Attacks on logon/password systems

Due to their inherent weaknesses, logon-ID/password access control technique is vulnerable to various kinds of malicious attacks. Some of the common attacks on such systems are discussed below:

- **Brute force:** In this crude form of attack, the attacker tries out every possible combination to hit on the successful match. The attacker may also use various password cracking software that assist in this effort.
- **Dictionary attack:** On the similar lines as brute force, this type of attack is based on the assumption that users tend to use common words as passwords, which can be found in a dictionary, hence the name. The "dictionary" simply consists of a list of words, including proper names (Raju, Ramesh, Ibrahim, etc.) and also that of mythological or religious names (Krishna, Jesus, Osiris, Buddha, etc.).

- **Trojan:** A malicious software, which the attacker can use to steal access control lists, passwords or other information.
- **Spoofing attacks:** In this technique, the attacker plants a Trojan programme, which masquerades as the system's logon screen, gets the logon and password information and returns control to the genuine access control mechanism. Once the information is obtained, the attacker uses the information to gain access to the system resources.
- **Piggybacking:** As stated earlier, an unauthorised user may wait for an authorised user to log in and leave a terminal unattended. The logical techniques that are used to secure against this attack are to automatically log out the session after a pre-determined period of inactivity or by using password-protected screen savers.

Token Based Authentication

Objects that a user is required to possess for identification and authentication are known as tokens.

(i) **Plastic Cards:** Plastic cards contain information about the user and primarily provide a means of identification of the user and can enable authentication. Plastic cards can further be of the following types:

- Memory tokens: In its most common form, the cards contain visible information such as name, identification number, photograph and such other information about the user and also a magnetic strip. This magnetic strip stores static information about the user. In order to gain access to a system, the user in possession of a memory token may be required to swipe his card through a card reader, which reads the information on the magnetic strip and passes onto the computer for verification with stored information to enable access. E.g. Employee badges with encoded magnetic strips. Where two-factor authentication is adopted, the user is not only required to have his card read by a card reading device but also required to key in remembered information (passwords, PIN) to gain access to the system resources. E.g. Bank ATM Card.

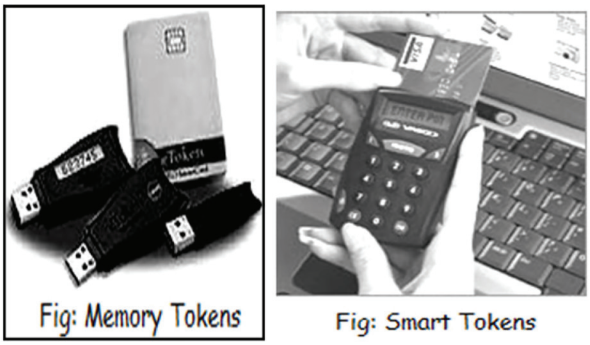


Fig: Memory Tokens

Fig: Smart Tokens

Figure 5.9 Tokens

- **Smart Tokens:** In this case, the card or device contains a small processor chip which enables storing dynamic information on the card. Besides static information about the user, the smart tokens can store dynamic information such as bank balance, credit limits etc., however the loss of such smart cards can have more serious implications.

(ii) **Proximity Readers:** In this case when a person in possession of the card reaches the restricted access area, the card data is read by the proximity readers (or sensors) which transmits information to the authentication computer, which enable access to the restricted area or system. The advantages are that the user is not required to insert the card into the device hence access time is faster. Proximity tokens can be either static or processor based. In static tokens, the card contains a bar code, which has to be brought in proximity of the reader device. In case of processor based tokens, the token device, once in the range of the reader, senses the reader and transmits a series of codes to the reader. Other token based systems include challenge response systems and one time passwords.

(iii) **Single Sign-on:** In many organisational situations, one user, by virtue of his job responsibilities is often required to log into more than one application. This raises the complex issue of multiple logon and passwords, for the user to remember. This is often solved by a single sign-on, which enables user access to various applications entitled for access. It is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The single sign-on, which is requested at the initiation of the session, authenticates the user to access all the applications they have been given the rights to on the server, and eliminates future authentication prompts when the user switches applications during that particular session. This often requires transferring all login control to an access control system, careful configuration of authorities, strong passwords and adequate security of password information since compromise of a single login giving access to multiple applications can lead to many systems being compromised. The concern in a decentralized processing or database environment is that the passwords travel over communication lines. Also if the single username and password used for single sign on is compromised, unauthorised access to all related application is possible.

5.8.5 Biometric Security

Biometrics offers a very high level of authentication based on “what the user is”, as compared to logon and token based authentication. Biometrics as the name suggests is based on certain physical characteristics or behavioural patterns identified with the individual, which are measurable. The International Biometric Group defines biometrics as automated mechanism which uses physiological and behavioural characteristics to determine or verify identity and further explains that the physiological biometrics are based on measurements and data derived from direct measurement of a part of the human body. Behavioural biometrics are based on measurements and data derived from an action and indirectly measure characteristics of the human body based on some feature unique to every user, biometrics seek to minimise the weaknesses in other mechanisms of authentication. Some of the biometric characteristics which are used are:

- Fingerprint
- Facial Scan
- Hand Geometry
- Signature
- Voice

- Keystroke Dynamics
- Iris Scanners
- Retina Scanners

Implementation of biometric authentication is often expensive and involves the following phases:

- Identification of IS assets which require biometric security
- Based on the above, identification of appropriate biometric application
- Acquisition and Testing of appropriate hardware, calibration of error rates for effectiveness and efficiency of enrolment and readability
- Implementation of administrative procedures for exception reporting and adjustment for false positives
- Enrolment of Users
- Implementation of related physical and logical controls

Identification and authentication is based on a match with items in the database containing data captured during the user enrolment. Registration or enrolment of the individuals' physical or behavioural characteristics involves capture of information, digitizing and storage of the biometric data. Based on the data read by the sensor, the image or digitized data is compared to the stored data to obtain a match. If the match succeeds, authentication is successful. However due to the complexity of data, biometrics suffer from two types of error viz. False Rejection Rate (FRR) which is wrongfully rejecting a rightful user and False Acceptance Rate (FAR) which involves an unauthorised user being wrongfully authenticated as a right user. Ideally a system should have a low false rejection and low false acceptance rate. Most biometric systems have sensitivity levels which can be tuned. The more sensitive a system becomes, FAR drops while FRR increases. Thus, FRR and FAR tends to inversely related. An overall metric used is the Crossover Error Rate (CER) which is the point at which FRR equals FAR.

Due to their high cost of implementation, biometric access controls were initially implemented only for high value critical information resources such as defence, banking etc. However with the rapid decrease in the cost of biometric hardware biometric controls are being increasingly preferred for commercial applications. Finger print based biometric controls are quite popular and widely deployed in data centres.

5.8.6 Authorisation Techniques: Operating Systems

Operating systems are fundamental to provide security to computing systems. The operating system supports the execution of applications and any security constraints defined at that level must be enforced by the operating system. The operating system must also protect itself because compromise would give access to all the user accounts and all the data in their files. A weak operating system would allow attackers access not only to data in the operating system files but data in database systems, if any, that use the services of the operating system. The operating system isolates processes from each other, protects the permanent data stored in its files, and provides controlled access to shared resources. Most operating systems use the access matrix as security model. An access matrix defines which processes have what types of access to specific resources.

General operating systems access control functions include:

- Authentication of the user
- User Management
- Restrict Logon IDs to specific workstations and/or specific times
- Manage account policies
    - o Password Policy
    - o Account Lockout Policy
- Manage audit policy
- Log events and report capabilities

5.8.7 Pluggable authentication modules

The pluggable authentication module (PAM) framework provides system administrators with the ability to incorporate multiple authentication mechanisms into an existing system through the use of pluggable modules. Applications enabled to make use of PAM can be plugged-in to new technologies without modifying the existing applications. This flexibility allows administrators to do the following:

Select any authentication service on the system for an application

- Use multiple authentication mechanisms for a given service
- Add new authentication service modules without modifying existing applications
- Use a previously entered password for authentication with multiple modules
- A general authentication scheme independent of the authentication mechanism may be used.

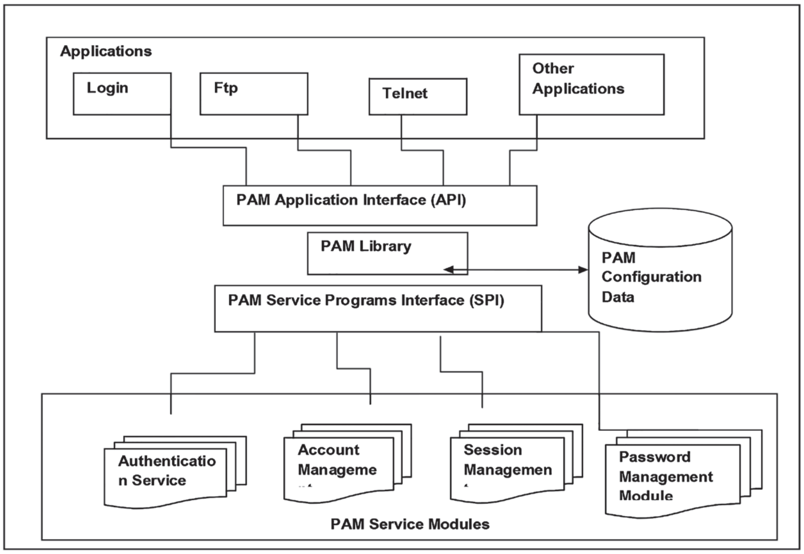


Figure 5.10: PAM Framework

5.8.8 File permissions

In most operating systems, every file is owned by a user and can be accessed by its owner, group or public, depending upon access permissions. When a user creates a file or directory, that user becomes the default owner of that file or directory. A user may be member of one group or many groups. Further, a user owner of a file may not be part of the group that also may have access to the file. Again, most operating systems have at least three types of file permissions; read, write and execute. The users have to be given at least read access to many of the system files.

5.9 Access Control Lists (ACL)

An access control list is a table that tells the computer operating system which access rights each user has to a particular system object, such as a directory/folder or an individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with his access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program). The access control list is implemented differently by each operating system and is the foundation of any security functionality. Access control enables one to protect a system or part of the system (directories, files, file types, etc.). When the system receives a request, it determines access by consulting a hierarchy of rules in the ACL. ACL has one or more access control entries (ACEs), each consisting of the name of a user or a group of users. The user can also be a role name, such as programmer or tester. For each of these users, groups, or roles, the access privileges are stated in a string of bits called an access mask. Generally, the system, administrator or the object owner creates the access control list for an object.

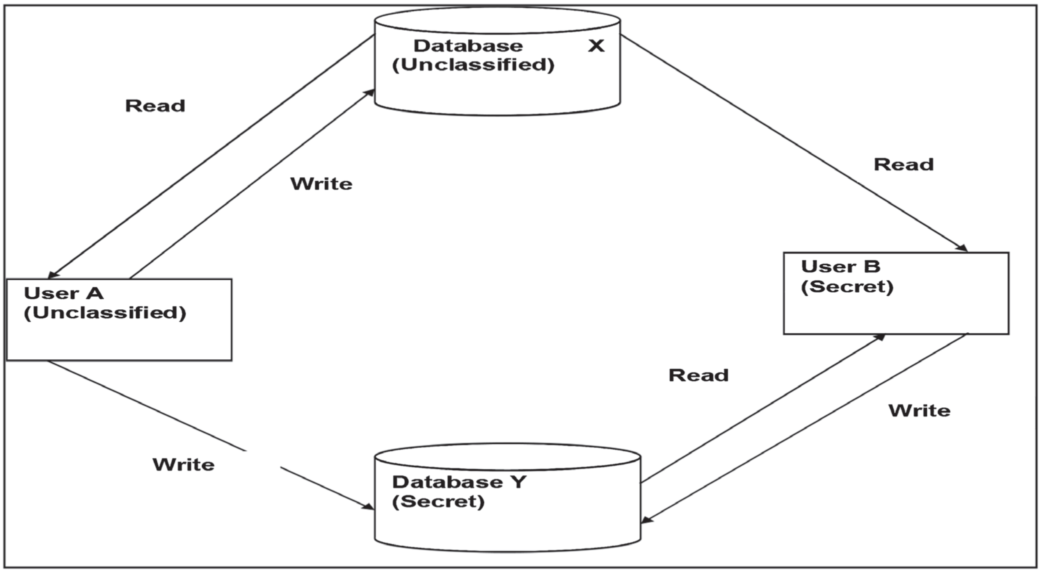


Figure 5.11: Read and Write Access Policy

Discretionary access privileges to user's poses problems within the organisation therefore the need arise to have a mandatory and well documented access control policies. Access control policies use attributes to determine which user can access which resource. An example access policy implementation here allows both the user A and User B can read from the unclassified database, but the secret database can be read only by the secret user B. Suppose if both the user A and user B can write to the unclassified and secret database then the unclassified user can read the secret information written by the secret user B and hence the user B has been responsible in downgrading the information.

User	Resource	Database X	Database Y
User A		Read & Write	Write
User B		Read	Read & Write

5.10 Identity Management and Access Controls

Identity Management, also called *IDAM*, is the task of controlling the User Access Provisioning Lifecycle on Information Systems. It includes the task of maintaining the identity of a user, actions they are authorized to perform. It also includes the management of descriptive information about the user and how and by whom that information can be accessed and modified.

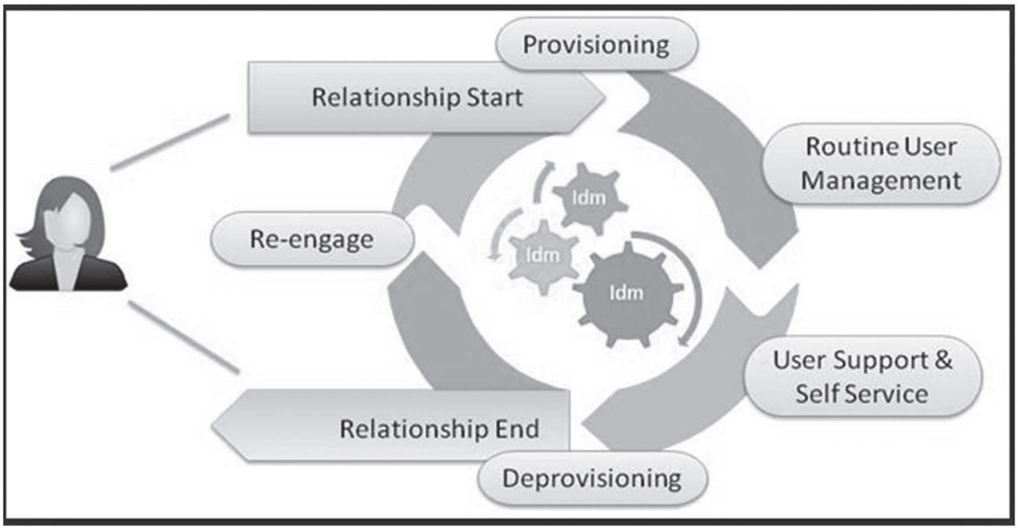


Figure 5.12: Components of identity management

The core objective of an IdM system in a corporate setting is: one identity per individual. And once that digital ID has been established, it has to be maintained, modified and monitored throughout what is called the "User access lifecycle." So IdM systems provide administrators with the tools and technologies to change a user's role, to track user activities and to enforce policies on an ongoing basis. These systems are designed to provide a means of administering user access across an entire enterprise and to ensure compliance with corporate policies and regulatory requirements like Sarbanes Oxley.

5.11 Privileged logons

Privileged user is a user who has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and Network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users.

Privileged access should be assigned based upon function and job necessity and are subject to approval by the information owner. All Users that have access to privileged accounts should be assigned their own user ID for normal business use. Privileged Users must use their personal user IDs for conducting non-privileged activities. Wherever possible the User must login to a system using their personal user ID prior to invoking a privileged account. Privileged Users should be required to create strong passwords comprising of letters, numbers, and special characters. The user account that has privileged access should have a unique password that is different from all other accounts accessed by the User.

5.12 Bypass Security Procedures

Bypass, in general, means either to go around something by an external route rather than going through it, or the means of accomplishing that feat. In network security, a bypass is a flaw in a security system that allows an attacker to circumvent security mechanisms to get system or network access. The actual point of entry is through a mechanism (either a hardware device or program, even just a piece of code) that enables the user to access the system without going through the security clearance procedures (such as authentication) that were set up by the system administrator. A bypass may be a mechanism put in place by an attacker, a flaw in the design, or an alternate access route left in place by developers. A bypass that is purposefully put in place as a means of access for authorized users is called a *back door* or a *trap door.* A crypto bypass is a flaw that allows data to circumvent the encryption process and escape, unencrypted, as plaintext.

5.13 The Access control Matrix

The access matrix provides access rights to subjects for objects. Access rights are of the type read, write, and execute. A subject is an active entity that is seeking rights to a resource or object. A subject can be a person, a program, or a process. An object is a passive entity, such as a file or a storage resource. A typical access control matrix is shown in Table 5.1 here.

Table 5.1: Example of an access matrix

	Object		
Subject	Customer Master File	Salaries File	Print Server
Ajay	Read	Read/Write	Write
Deepak	Read/Write	Read	Write
Ram	Read	Read	None

The columns of the access matrix are called *Access Control Lists (ACLs),* and the rows are called *capability lists.* The access matrix model supports discretionary access control because the entries in the matrix are at the discretion of the individual(s) who have the authorisation authority over the table.

5.13.1 User of Generic / Group IDs

Many a time to maintain continuity group users IDS are created and password is shared among select users. This generally happens in case of administrator group. The main concern in using group id is the fixing accountability of actions to individual. However organisation may implement manual controls to achieve this. IS auditor must review the effectiveness of such controls. However use of generic accounts like temp or guest should not be allowed, unless specifically approved by Information Security Officer, assigned to an individual and documented. It should have an owner accountable for all actions performed using that ID. These days, many ERP vendors (including SAP) don't permit creation and use of generic/group accounts and is clearly documented in the licensing agreement. Besides, users should not be allowed to share their user IDs with others.

5.14 Single Sign-On (SSO)

Single Sign-On addresses the practical challenge of logging on multiple times to access different resources. A user must remember numerous passwords and IDs and might take shortcuts in creating passwords that might be open to attack. In SSO, a user provides one ID and password per work session and is automatically logged on to all the required applications. For SSO security, the passwords should not be stored or transmitted in the clear. SSO can be implemented by using scripts that replay the users' multiple logins or by using authentication servers to verify a user's identity and encrypted authentication tickets to permit access to system services.

The advantages of SSO include having the ability to use stronger passwords, easier administration of changing or deleting the passwords, and requiring less time to access resources. The major disadvantage of many SSO implementations is that once a user obtains access to the system through the initial logon, the user can freely roam the network resources without any restrictions. There are multiple methods used by organisations to implement single sign-on. Most popular being LDAP (Open Source) and Active Directory (AD) (Microsoft directory service based on LDAP) where user groups and roles are defined for every user and accesses are granted based on access control matrix. There are some applications like Kerberos are also available

5.14.1 Active Directory (AD)

AD is a directory service implemented by Microsoft for Windows domain networks. It is included in most Windows Server operating systems. An AD domain controller authenticates and authorises all users and computers in a Windows domain type network-assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user. Active Directory makes use of Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.[1] Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organised set of records, often with a hierarchical structure, such as a corporate e-mail directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number. A common usage of LDAP is to provide a "single sign on" where one password for a user is shared between many services, such as applying a company login code to web pages (so that staff log in only once to company computers, and then are automatically logged into the company intranet)

5.14.2 Kerberos

Kerberos may be one of the best-tested authentication mechanism available today. Kerberos was intended to have three elements to guard a network's entrance: ***authentication, accounting,*** and ***auditing.***

Kerberos is effective in open, distributed environments where network connections to other heterogeneous machines are supported and the user must prove identity for each application and service. Kerberos assumes a distributed architecture and employs one or more Kerberos servers to provide an authentication service. This redundancy can avoid a potential single point of failure issue. The primary use of Kerberos is to verify that users are who they claim to be and the network components they use are contained within their permission profile. To accomplish this, a trusted Kerberos server issues "tickets" to users. These tickets have a limited life span and are stored in the user's credential cache.

5.14.3 Weakness of Single Sign-on

SSO has a number of weaknesses that can make it vulnerable to attack. Some of these are:

- It is a single point of failure. One password is compromised, and attacker can have access to all privileges of users whose password is compromised.
- Vulnerable to password guessing.
- Does not protect network traffic.
- When a user changes password, SSO database needs to be updated with a new corresponding password.
- It is difficult to implement when organisation has legacy applications or applications that cannot be plugged in with SSO.
- Maintaining SSO is tedious and prone to human errors.

5.14.4 Authorisation

SSO system knows who user is (authentication) and must now decide if user can carry out the requested actions. This is where authorisation comes into play. Authorization determines what the user is allowed to do. Once a user's identity and authentication are established, authorisation levels determine the extent of system rights that a user can hold.

Access criteria types can be broken up into:

- Roles
- Groups
- Physical or logical (network) location

- Time of day
- Transaction type

All access criteria should default to “no access” and authorisations should be granted on need to know basis. Just because a subject has been identified and authenticated does not automatically mean they have been authorised. It is possible for a subject to be logged onto a network (i.e., identified and authenticated) but be blocked from accessing a file or printing to a printer (i.e., by not being authorized to perform that activity). Most users are authorized to perform only a limited number of activities on a specific collection of resources. Identification and authentication are all-or-nothing aspects of access control. Authorization has a wide range of variations between all or nothing for each individual object within the environment. A user may be able to read a file but not delete it, print a document but not alter the print queue, or log onto a system but not access any resources.

5.15 Access Controls in Operating Systems

This topic covers how authorization mechanism is applied to subjects and objects. ***Subject*** of operating systems are (active) entities that communicate with the system and use its resources. The best example for a subject is the user or a process. ***Objects*** on the other hand are entities of the operating system that are accessed (requested) by the subject. The access control mechanism should ensure that subjects gain access to objects only if they are authorized to. Depending on areas of usage, there are three types of access control used:

- **Mandatory Access Control–** It is a multi-level secure access control mechanism. It defines a hierarchy of levels of security. A security policy defines rules by which the access is controlled.
- **Discretionary Access Control–** In this type of access control, every object has an owner. The owner (subject) grants access to his resources (objects) for other users and/ or groups. The matrix defines the whole state of the system concerning the rights of individual users. There are two ways how to implement the matrix. Either the system assigns the rights to the objects or to the subjects. In other words, either the object stores the column of the matrix, or the subject stores the row of the matrix. Access control lists are used to store the rights with object. On the other hand capability matrixes are used to store rights together with subjects. In the case of capability matrixes we would have to deal with biometrics, so in common operating systems access control lists are used to implement discretionary access control.
- **Role Based Access Control–** In some environments, it is problematical to determine who the owner of resources is. In role based systems, users get assigned roles based on their functions in that system. These systems are centrally administered, they are non-discretionary. An example is a hospital.

5.16 Database Controls

One of the important objectives of access controls is to prevent any threats to the integrity and unauthorised access to the database resources. Relational Database works on the principles of tables and relations and allows rules of integrity and access to be specified. The principle of least privileges to data items can be enforced using views as against reads. Such rules can be restricted by a range of parameters such as permissible values or limits, operations up to the granularity of a data field etc. The access to data base can be **Discretionary** based on the approved by data owner (usually business process owner who is accountable for data stored in database), and **Mandatory**. DBA may use various methods to implement access controls in database like depending upon role of user, access control matrix, classification of data item (for example credit card and password stored in database must be encrypted) mapped with roles and so on. Access to SQL and schema level are generally restricted to DBA or implemented through application controls.

5.16.1 Database Roles and Permissions

Access to database can't be controlled through the permission settings. This can be useful when it is needed to:

- Share confidential information with other managers, but not the entire company.
- Allow all team members to enter and update issues in an issue tracking database.
- Post a widely referenced database such as a job postings database, but allow only a few people to edit.

Each database has its own customisable permissions system. The permission system is based on *access levels.* Each user of a database has an access level that controls what that user is allowed to do. For example, a user with Read access is only allowed to view information in the database, not change any of it. A user with Edit access can view and change information.

Table 5.2: Database access level

Access Level	Rights
No Access	Users can neither see nor use the database.
Read	Users can view any existing information and can use export to save that information to a file. They cannot add new information to the database, nor can they use import to create new information. They also cannot edit or delete existing information in the database. Users cannot edit the design of the database.
Read & Add	Users can view any existing information and can use export to save that information to a file. They can add information to the database either manually or by importing information from a file. Users with Read & Add access can only edit or delete information they added. They cannot change any information added by other users. Users cannot edit the design of the database.
Read & Add (Own Records Only)	Users can add information to the database either manually or by importing information from a file. Users can only view information they added. They can also edit, delete or export the information they added. They cannot view, edit, delete or export information added by other users. Users cannot change any details of the database design.

Edit	Users can view any existing information and can use export to save that information to a file. They can add information to the database either manually or by importing information from a file. Users can edit and delete any information in the database. They cannot change any details of the database design.
Manage	Users can view, edit, add, and delete any information in the database and any aspect of the database design. They can also export any information to a file, and import information from a file. A member who has Manage access is called a *Database Manager.* This is a powerful permission level, so use it carefully.

When a database is created, the Database application automatically gives the owner Manage access and everyone else No Access. DBA the use ***database roles*** to more easily manage privileges for groups of users. Database roles simplify the process of managing privileges because DBA can grant privileges to a role, and then grant the role to users. When owner wants to revoke privileges for a user, he/she can simply revoke role authorisation from the user, rather than revoking each individual privilege. He/she can create and drop a role by using the same process that he would to make any database object change. Generally, there are two types of database-level roles: ***fixed database roles*** that are predefined in the database and ***flexible database roles*** that an owner can create.

5.16.2 Application Software Controls in a Database

Access to database and fields can be controlled through application thus eliminating need to create users at data base level or these users are mapped with application level users. Accesses are then granted within application and user can access data only through application. For example if a user role requires access to a report, a view can be created and assigned to application module/menu. User then provided access to the menu. Integrity of a DBMS system depends in part on the controls implemented in the application programs that provide the interface to the user to perform a job process activity with a sequence of commands and update parameters that are passed with respect to certain considerations or actions.

Direct access to database level (also sometimes referred as backend access) are then restricted only to data base administrators (DBA) to perform maintenance work. It is possible to restrict DBA to access data.

5.17 Audit of Access Controls

Some factors critical to the successful achievement of audit objectives with regard to evaluating logical access are:

- The *understanding of an organisation's* information security framework, security policy linkage of IT objectives to its business objectives and assessment of risk and controls. This often forms the foundation for risk management and criteria for determining the amount of investment and philosophy of access controls.
- *Selection and implementation of appropriate access controls* should be consistent with the organisation's structure, management controls and organisational culture.

- *Top management's commitment,* support and control must be communicated to all levels in the organisation and concerned stakeholders. Management support would be evident from the emphasis and investment on training and education of users, the importance given to access controls and the enforcement of access control discipline.
- *Management controls* should be evaluated to determine if adequate systems are in place. This also helps to detect report and take corrective action on access security violation.
- Access to all Systems should be granted in a controlled manner driven by business requirements. Users should be explicitly granted access to information or systems. There is no implicit right of access. Access is denied unless explicitly permitted.
- User access rights should be reviewed / audited periodically by the information owners and user access should be revoked based upon their request. This should include audit/ review of privileged / super user access rights.
- User accounts that have not been accessed for a predetermined number of days should be disabled in accordance with company's records retention guidelines.

The auditor's opinion depends on his understanding of general and IS controls and audit procedures. These are used to test the effectiveness and efficiency of access to organisational information, in respect of which the auditor should exercise due care and diligence.

The objective and scope of audit would determine the audit procedures and IS resources to be covered. Often evaluation of logical access controls forms a part of a generic IS audit covering various other controls. However, the auditor may be required to evaluate the logical access security of a system, sub-system, application, operating software, database management software.

5.17.1 Audit Test Procedures

IS auditors should evaluate whether logical access policies and procedures are effectively implemented. For this the auditor has to test if:

- Necessary access control framework in the form of logical access security policies and standards are in place and effectively communicated. The auditor does this by studying the various policies, the system of communication of policy initiatives and the system of education and training users with respect to logical security of information resources. The auditor would need to interview data owners, users and custodians to evaluate their knowledge and skills on implementation of access controls.
- Procedures and mechanisms for logical access are implemented to ensure protection of organisational information. The IS auditor should evaluate the various logical security techniques and mechanisms for their effective implementation, operation and administration.
- The auditor must check if the controls are functioning effectively and efficiently. This requires the auditor to conduct various compliance and substantive tests to determine if the logical security of information resources is actually effective. The auditor can determine the level of effectiveness of logical security by determining compliance with procedure manuals such as administrator manuals and user manuals, interviewing users and administrators and testing the various logical security mechanisms to determine any weaknesses or incompatibilities.

Some audit considerations in this regard are outlined in next section.

5.17.2 Logical access: Audit considerations

Following considerations must be considered while reviewing logical accesses.

1. System Configuration
2. Logical access mechanism
3. Bypass security procedures

5.17.3 Systems Configuration

Test the appropriateness of system configuration and parameter settings. Appropriate configurations of access security parameter systems at the time of installing/ upgrading hardware, system software such as operating systems, DBMS and application software are critical in building a strong foundation for access security. In this respect the auditor would have to evaluate whether:

- The system configuration complies with the organisational security standards, security policy requirements, manufacturer specifications and best practices for security.
- There is a process to ensure that configuration of access security settings and parameters and changes thereto are authorised, documented and tested.
- Privileged and special purpose logons are controlled and documented.
- There is a procedure for control over purchase, custody and management of system utilities. Many systems utilities are powerful and can break through the various levels of access security.

5.17.4 Logical Access mechanisms

For testing of various logical access mechanisms such as token based authentication systems and biometric access control systems the auditor can conduct tests that determine:

- The control of authorisation, operation and termination over use of tokens such as memory and smart cards.
- Control over special terminals and devices. For instance, a hub may be exposed physically but with proper levels of encryption, logical security of information can be ensured.
- Security practices relating to unattended terminals, security of data in transit and control over production resources.
- Whether logging of transactions and events is appropriately enabled.

User account management and password management

Logon and passwords are the most commonly used mechanisms to secure logical access to information resources. The auditor should:

- Evaluate mechanisms such as access control features and software to identify weaknesses if any.

- Evaluate the effectiveness of user management procedures through audit of access control lists to assess if access is permitted based on the principle of least privileges and "need to know-need to do" basis, scan audit logs to determine the effectiveness of access control and interview users, and identify all entries in ACL with the authorised list of employees permitted to access systems.
- Test user profiles and group profiles to determine the access privileges and controls thereon.

Privileged logons and special user accounts

Privileged logons and special user accounts provide higher level of access to systems resources. Hence, they require a higher level of access security and management. The auditor should evaluate:

- The strength of controls on such privileged access. He should follow appropriate audit procedures to identify all individuals having access to such privileged logon facility and special user accounts. The auditor should critically evaluate the need for such access
- Review audit trails, access violation reports in respect of all privileged logons and special user accounts
- The strength and adequacy of monitoring and incident handling procedures

Access to file directories and application logic and system instruction sets

The auditor should evaluate the protection of :

- Systems files and directories containing critical hardware and systems software configuration and parameter files such as driver information, etc.
- Application files and directories containing application programmes, support files, programme libraries, parameter files, initialisation files, etc.
- Production data and directories containing production files and production resources.

5.17.5 Bypass Security Procedures

There may be various situations in the routine course of operations where security features are bypassed for operational and functional convenience during certain controlled operations. For instance, privileged logons may be provided to systems engineers to meet emergency situations, bypass label processing may be provided to meet certain bulk processing requirements or systems exits may be enabled during software implementation and maintenance phases. The auditor should identify all such provisions and critically audit the events.

5.18 Summary

When deciding on a logical access control strategy, it is important to review compliance and internal security requirements necessary to protect access to information assets. This can best be achieved by conducting a risk analysis that identifies the typical threats. In addition inputs from global standards are also useful. Most important consideration is identifying users, type of access, and type of asset. It best to adopt a least privilege policy on "need to know, need to do" basis. After answering these questions, it is possible to plan for a combination of access controls necessary to meet the security goals.

Auditor should know that access control defines how users should be identified, authenticated, and authorized. This is generally addressed in Security policies and procedures, hence the starting point of audit of logical access controls should be to understand the policies and procedures and ensure these are implemented uniformly and continuously.

5.19 Questions

1. Which of the following pair of authentication can be considered as two factor?
   - A. Password and passphrase
   - B. Passphrase and PIN
   - C. Token and access card
   - D. Access card and PIN
2. Which of the following is primary requirement of granting user access to information asset?
   - A. Identification
   - B. Authorisation
   - C. Authentication
   - D. Need to know
3. Mandatory access controls are those controls that are:
   - A. Based on global standards
   - B. Defined by security policy
   - C. Part of compliance requirements
   - D. Granted by asset owner
4. Which of the following is a major concern associated with Single-Sign-on?
   - A. Multiple passwords are noted
   - B. User may select easy password
   - C. It is a single point of failure
   - D. High maintenance cost
5. Which of the following non-compliance with security policy is most difficult to detect or get evidence for?
   - A. Use of removable media
   - B. Password sharing by user
   - C. Access to banned web sites
   - D. Passing information over phone

6. Which of following processes in user access management is most essential to detect errors and omissions resulting in unauthorised or excess accesses to users?

   A. Identification

   B. Authentication

   C. Authorisation

   D. Review

7. While auditing compliance with password policy, IS auditor observed that configuration of password parameters in system is as per policy. Which of the following the auditor should verify?

   A. Review enforcement for sample users.

   B. Verify all assets have same configuration.

   C. Review log for password configuration.

   D. Interview users on policy enforcement.

8. One time password is considered strong because they are:

   A. Active for short period.

   B. Communicated on mobile.

   C. Unique for each user

   D. Unique for session

9. Which of the following has been attack to break the user password is difficult to control?

   A. Brute Force

   B. Dictionary attack

   C. Spoofing

   D. Social engineering

10. Which of the following is a primary objective of implementing logical access controls?

    A. Identify users on the system

    B. Fixing accountability of actions

    C. Authorise users based on role

    D. Compliance with policy

5.20 Answers and Explanations

1. D.The three factors are what a user knows (PIN, Password, Passphrase), what user possesses (Access card, Token) and what unique characteristics of user (Biometric) are. Use of any two factors for authentication is called two factor. Option A, B and C though strong use only one factor.
2. A.Identification of user is first and primary requirement of granting access. Next will be authentication method to be established and finally finding authorisation levels based on role that also addresses need to know.
3. B. Mandatory accesses are those controls that are to be applied uniformly across organisation and are defined by security policy. D is discretionary access controls. A and C generally do not specify such requirements.
4. C. Single point of failure is a major concern. One password if compromised, all accesses for that user are available to perpetrator.
5. B. Password sharing by user is most difficult to get evidence for or detect. Others can be monitored or enforced using technology.
6. D. Periodic user access review helps in ensuring that all users have appropriate level of accesses. This happens due to changes in internal environment like role changes, emergency situation, resignation and retiring of employees. In such situations sometimes revocation of accesses is missed out, and can be corrected during review.
7. C. Generally automated configuration need not be reviewed for samples except for sample assets. However it is most important to review the password configuration changes for ongoing enforcement of policy.
8. A. Strength of one-time password is that they are active for short time, if user does not login during that time the password expires. Password is unique for each session and user, however it is not a strength. It can be communicated by suitable means.
9. D. Social engineering attacks weakest link that is human. Attacker uses techniques to compel users to reveal passwords and other confidential information. For example Phishing. Other options are technology based attacks and can be detected or controlled.
10. B. Primary objective of implementing access controls is to fix accountability on user for their actions. Others are means to implement access controls not objectives.

CHAPTER 6: NETWORK SECURITY CONTROLS

6.1 Introduction

We have seen the use of networks for business communication and application hosting in Module 1, in this section, we will review the risks and controls that are specific to networked computers. It is rare these days to find a standalone computer in any commercial environment, as networks offer tremendous advantages that far outweigh the cost of creating them. Although it is true that when we are implementing security controls it is necessary to focus on enterprise architecture as a whole for designing and implementing controls, network related controls are important since it is the first layer of architecture that is generally is focus of attacker. Therefore networks are also far more vulnerable to external and internal threats than are standalone systems.

Organisation level general controls like physical security (cables, intruders trying to connect to network), environmental security (ensuring segregation between electrical and data cables, protecting cables from rodents), access controls, security policies (acceptable usage of internet) are applicable to network security. In addition one needs to look at network specific controls to ensure that organisation's security objectives are achieved.

6.2 Network Characteristics

Advantages of enterprise wide network characteristics are described as the following:

- **Anonymity:** A network removes personal interaction i.e. most of the clues, such as appearance, voice, or context, by which we recognise acquaintances.
- **Automation:** In some networks, one or both endpoints, as well as all intermediate points, involved in a given communication may be machines with only minimal human supervision.
- **Distance:** Many networks connect endpoints that are physically far apart. Although not all network connections involve distance, the speed of communication is fast enough that humans usually cannot tell whether a remote site is near or far. Though it makes it easier to establish communication among geographically dispersed users/machines, it also introduces risks like impersonation, intrusion, tapping.
- **Opaqueness:** Because the dimension of distance is hidden, users cannot tell whether a remote host is in the room next door or in a different country. In the same way, users cannot distinguish whether they are connected to a node in an office, school, home, or warehouse, or whether the node's computing system is large or small, modest or powerful. In fact, users cannot tell if the current communication involves the same machine with which they communicated the last time.
- **Routing diversity:** To maintain or improve reliability and performance, routings between two endpoints are usually dynamic. That is, the same interaction may follow one path through the network the first time and a very different path the second time. In fact, a query may take a different path from the response that follows a few seconds later.

6.3 Threats and Vulnerabilities

This section describes the various kinds of vulnerabilities and threats associated with networks that aim to compromise the confidentiality, integrity, or availability of data, software and hardware by accidents, non-malicious humans, and malicious attackers. The threats and vulnerabilities are listed under the following heads:

- Information Gathering
- Communication Subsystem Vulnerabilities
- Protocol Flaws
- Impersonation
- Message Confidentiality Threats
- Message Integrity Threats
- Web Site Defacement
- Denial of Service

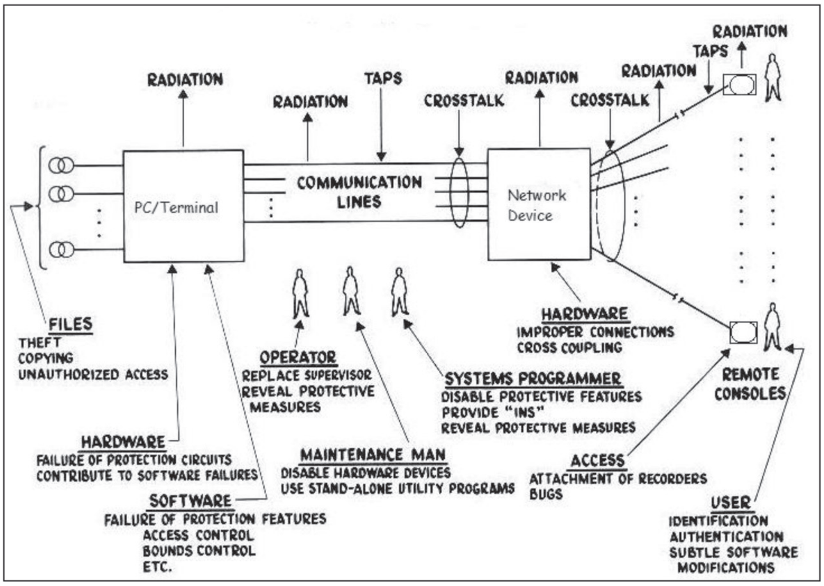


Figure 6.1 Network Vulnerabilities

However it needs to be understood that most of these threats operate in tandem and it is difficult to associate them with network security alone. Figure 6.1 illustrates the various threats in and their source or initiator. This will help auditors in understanding types of threat that might materialise in which part of IT installation and verify controls for those threats, based on risk assessment results.

6.3.1 Information Gathering

A serious attacker will spend a lot of time obtaining as much information as s/he can about the target before launching an attack. The techniques to gather information about the networks are examined below:

- **Port Scan:** An easy way to gather network information is to use a port scanner, a programme that, for a particular IP address, reports which ports respond to messages and which of several known vulnerabilities seem to be present.
- **Social Engineering:** Social engineering involves using social skills and personal interaction to get someone to reveal security-relevant information and perhaps even to do something that permits an attack. The point of social engineering is to persuade the victim to be helpful. The attacker often impersonates someone occupying a senior position inside the organisation and is in some difficulty. The victim provides the necessary assistance without verifying the identity of the caller, thus compromising security.
- **Reconnaissance:** Reconnaissance is the general term for collecting information. In security, it often refers to gathering discrete bits of information from various sources and then putting them together to make a coherent picture. One commonly used reconnaissance technique is "dumpster diving." It involves looking through items that have been discarded in garbage bins or waste paper baskets. One might find network diagrams, printouts of security device configurations, system designs and source code, telephone and employee lists, and more. Even outdated printouts may be useful. Reconnaissance may also involve eavesdropping. The attacker or his accomplice may follow employees to lunch and listen in from nearby tables as co-workers discuss security matters.
- **Operating System and Application Fingerprinting:** Here the attacker wants to know which commercial server application is running, what version, and what the underlying operating system and version are. While the network protocols are standard and vendor independent, each vendor has implemented the standard independently, so there may be minor variations in interpretation and behaviour. The variations do not make the software non-compliant with the standard, but they are different enough to make each version distinctive. How a system responds to a prompt (for instance, by acknowledging it, requesting retransmission, or ignoring it) can also reveal the system and version. New features also offer a clue, for example a new version will implement a new feature but an old version will reject the request. All these peculiarities, sometimes called the operating system or application fingerprint, can mark the manufacturer and version.
- **Bulletin Boards and Chats:** Underground bulletin boards and chat rooms support exchange of information among the hackers. Attackers can post their latest exploits and techniques, read what others have done, and search for additional information on systems, applications, or sites.
- **Documentation:** The vendors themselves sometimes distribute information that is useful to an attacker. For example, resource kits distributed by application vendors to other developers can also give attackers tools to use in investigating a product that can subsequently be the target of an attack.
- **Malware:** Attacker may use malware like virus or worms to scavenge the system and keep sending information to attacker over network without the knowledge of system user.

6.3.2 Exploiting communication subsystem vulnerabilities

- **Eavesdropping and Wiretapping:** An attacker can pick off the content of a communication passing in unencrypted form. The term eavesdrop implies overhearing without expending any extra effort. For example, an attacker (or a system administrator) is eavesdropping by monitoring all traffic passing through a node. (The administrator might have a legitimate purpose, such as watching for inappropriate use of resources.) A more hostile term is wiretap, which means intercepting communications through some effort. Passive wiretapping is just “listening,” just like eavesdropping. But active wiretapping means injecting something into the communication stream. A wiretap can be done in such a manner that neither the sender nor the receiver of a communication will know that the contents have been intercepted.
- **Microwave signal tapping:** Microwave signals are broadcast through the air, making them more accessible to outsiders. An attacker can intercept a microwave transmission by interfering with the line of sight between sender and receiver. It is also possible to pick up the signal from an antenna located close to the legitimate antenna.
- **Satellite Signal Interception:** In satellite communication, the potential for interception is even greater than with microwave signals. However, because satellite communications are heavily multiplexed, the cost of extracting a single communication is rather high.
- **Wireless:** Wireless networking is becoming very popular, but threats arise in the ability of intruders to intercept and spoof a connection. A wireless signal is strong for approximately 30 to 60 meters. A strong signal can be picked up easily. Wireless also has a second problem, the possibility of unauthorised use of a network connection, or a theft of service.
- **Optical Fibre:** It is not possible to tap an optical system without detection. Further optical fibre carries light energy, not electricity, which does not emanate a magnetic field as electricity docs. Therefore, an inductive tap is impossible on an optical fibre cable. However, the repeaters, splices, and taps along a cable are places at which data may be intercepted more easily than in the fibre cable itself.
- **Zombies and BOTnet:** BOTnets is a term (robotic network) used for virtual network of zombies. BOTnet operator launches malware/virus on system that once activated remains on system and can be activated remotely. This malware helps the BOTnet operator use the compromised system (Zombie) remotely with to launch attack or collect information. For example Zombies have been used extensively to send e-mail spam. This allows spammers to avoid detection and presumably reduces their bandwidth costs, since the owners of zombies pay for their own bandwidth.

6.3.3 Protocol Flaws

Internet protocols are publicly posted for scrutiny. Many problems with protocols have been identified by reviewers and corrected before the protocol was established as a standard. Despite this process of peer review, flaws exist in many of the commonly used protocols. These flaws can be exploited by an attacker. For example FTP is known to transmit communication including user ID and password in plain text.

6.3.4 Impersonation

In many instances, an easy way to obtain information about a network is to impersonate another person or process. An impersonator may foil authentication by any of the following means:

- **Authentication foiled by guessing:** Guess the identity and authentication details of the target, by using common passwords, the words in a dictionary, variations of the user name, default passwords, etc.
- **Authentication foiled by eavesdropping or wiretapping:** When the account and authentication details are passed on the network without encryption, they are exposed to anyone observing the communication on the network. These authentication details can be reused by an impersonator until they are changed.
- **Authentication Foiled by Avoidance:** A flawed operating system may be such that the buffer for typed characters in a password is of fixed size, counting all characters typed, including backspaces for correction. If a user types more characters than the buffer would hold, the overflow causes the operating system to by-pass password comparison and act as if a correct authentication has been supplied. Such flaws or weaknesses can be exploited by anyone seeking unauthorised access.
- **Non-existent Authentication:** Here the attacker circumvents or disables the authentication mechanism at the target computer. If two computers trusts each other's authentication an attacker may obtain access to one system through an authentication weakness (such as a guest password) and then transfer to another system that accepts the authenticity of a user who comes from a system on its trusted list. The attacker may also use a system that has some identities requiring no authentication. For example, some systems have "guest" or "anonymous" accounts to allow outsiders to access things the systems want to release to the public. These accounts allow access to unauthenticated users.
- **Well-Known Authentication:** Most vendors often sell computers with one system administration account installed, having a default password. Or the systems come with a demonstration or test account, with no required password. Some administrators fail to change the passwords or delete these accounts, creating vulnerability.
- **Spoofing and Masquerading:** Both of them are impersonation. Refer to Chapter on Logical Access Controls for details.
- **Session Hijacking:** Session hijacking is intercepting and carrying on a session begun by another entity. In this case the attacker intercepts the session of one of the two entities that have entered into a session and carry it over in the name of that entity. For example, in an e-commerce transaction, just before a user places his order and gives his address, credit number etc. the session could be hijacked by an attacker.
- **Man-in-the-Middle Attack:** A man-in-the-middle attack is a similar to session hijacking, in which one entity intrudes between two others. The difference between man-in-the-middle and hijacking is that a man-in-the-middle usually participates from the start of the session, whereas a session hijacking occurs after a session has been established. The difference is largely semantic and not particularly significant.

6.3.5 Message Confidentiality Threats

An attacker can easily violate message confidentiality (and perhaps integrity) because of the public nature of networks. Eavesdropping and impersonation attacks can lead to a confidentiality or integrity failure. Here we consider several other vulnerabilities that can affect confidentiality.

- **Misdelivery:** Message misdelivery happens mainly due to congestion at network elements which causes buffers to overflow and packets dropped. Sometimes messages are misdelivered because of some flaw in the network hardware or software. Most frequently, messages are lost entirely, which is an integrity or availability issue. Occasionally, however, a destination address will be modified or some router or protocol will malfunction, causing a message to be delivered to someone other than the intended recipient. All of these "random" events are quite uncommon. More frequent than network flaws are human errors, caused by mistyping an address.
- **Exposure:** The content of a message may be exposed in temporary buffers, at switches, routers, gateways, and intermediate hosts throughout the network; and in the workspaces of processes that build, format, and present the message. A malicious attacker can use any of these exposures as part of a general or focused attack on message confidentiality.
- **Traffic Analysis (or Traffic Flow Analysis):** Sometimes not only is the message itself sensitive but the fact that a message exists is also sensitive. For example, if a wartime enemy sees a large amount of network traffic between headquarters and a particular unit, the enemy may be able to infer that significant action is being planned involving that unit. In a commercial setting, messages sent from the president of one company to the president of a competitor could lead to speculation about a takeover or conspiracy to fix prices.

6.3.6 Message Integrity Threats

In most cases, the integrity or correctness of a communication is more important than its confidentiality. Some of the threats which could compromise integrity are by:

- Changing some or all of the content of a message
- Replacing a message entirely, including the date, time, and sender/ receiver identification
- Reusing (replaying) an old message
- Combining pieces of different messages into one false message
- Changing the apparent source of a message
- Redirecting a message
- Destroying or deleting a message

These attacks can be perpetrated in the ways already stated, including:

- Active wiretap
- Trojan horse
- Impersonation
- Compromised host or workstation

6.3.7 Web Site Defacement

Web site defacement is common not only because of its visibility but also because of the ease with which one can be done. Web sites are designed so that their code is downloaded and executed in the client (browser). This enables an attacker to obtain the full hypertext document and all programs and references programs embedded in the browser. This essentially gives the attacker the information necessary to attack the web site. Most websites have quite a few common and well known vulnerabilities that an attacker can exploit.

6.3.8 Denial of Service

Denial of Service (DoS) attacks lead to loss of network availability. The electronic threats are more serious and less obvious. Some of them are described below:

- **Connection Flooding:** This is the oldest type of attack where an attacker sends more data than what a communication system can handle, thereby preventing the system from receiving any other legitimate data. Even if an occasional legitimate packet reaches the system, communication will be seriously degraded.
- **Ping of death:** It is possible to crash, reboot or otherwise kill a large number of systems by sending a ping of a certain size from a remote machine. This is a serious problem, mainly because this can be reproduced very easily, and from a remote machine. Ping is an ICMP protocol which requests a destination to return a reply, intended to show that the destination system is reachable and functioning. Since ping requires the recipient to respond to the ping request, all the attacker needs to do is send a flood of pings to the intended victim.
- **Traffic Redirection:** A router is a device that forwards traffic on its way through intermediate networks between a source host's network and a destination's. So if an attacker can corrupt the routing, traffic can disappear.
- **DNS Attacks:** DNS attacks are actually a class of attacks based on the concept of domain name server. A domain name server (DNS) is a table that converts domain names like www.icai.org into network addresses like 202.54.74.130, a process called resolving the domain name or name resolution. By corrupting a name server or causing it to cache spurious entries, an attacker can redirect the routing of any traffic, or ensure that packets intended for a particular host never reach their destination.

6.3.9 Distributed Denial of Service

In distributed denial of service (DDoS) attack more than one machine are used by the attacker to attack the target. These multiple machines are called zombies that act on the direction of the attacker and they don't belong to the attacker. These machines have some vulnerability that can be exploited to use it to attack another machine. The attacker exploits vulnerabilities in multiple machines and uses them to attack the target simultaneously. In addition to their tremendous multiplying effect, distributed denial-of-service attacks are a serious problem because they are easily launched by using scripts.

6.3.10 Threats from Cookies, Scripts and Active or Mobile Code

Some of the vulnerabilities relating to data or programs that are downloaded from the server and used by the client are as follows:

- **Cookies:** Cookies are NOT executable. They are data files created by the server that can be stored on the client machine and fetched by a remote server usually containing information about the user on the client machine. Anyone intercepting or retrieving a cookie can impersonate the cookie's legitimate owner.
- **Scripts:** Clients can invoke services by executing scripts on servers. A malicious user can monitor the communication between a browser and a server to see how changing a web page entry affects what the browser sends and then how the server reacts. With this knowledge, the malicious user can manipulate the server's actions. The common scripting languages for web servers, CGI (Common Gateway Interface), and Microsoft's active server pages (ASP) have vulnerabilities that can be exploited by an attacker.
- **Active Code:** Active code or mobile code is a general name for code that is downloaded from the server by the client and executed on the client machine. The popular types of active code languages are Java, JavaScript, VBScript and ActiveX controls. Such executable code is also called applet. A hostile applet is downloadable code that can cause harm on the client's system. Because an applet is not screened for safety when it is downloaded and because it typically runs with the privileges of its invoking user, a hostile applet can cause serious damage.

6.3.11Malicious Code

Malicious code is the name used for any programme that adds to, deletes or modifies legitimate software for the purpose of intentionally causing disruption and harm or to circumvent or subvert the existing system's function. Examples of malicious code include viruses, worms, Trojan Horses, and logic bombs. Newer malicious code is based on mobile Active X and Java applets.

Viruses

A computer virus is a type of malware (programme) that attaches itself to a file and gets transmitted. When executed, it damages the infected system and also replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".

Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes. However, not all viruses carry a destructive payload or attempt to hide themselves-the defining characteristic of viruses is that they are self-replicating computer programmes which install themselves without the user's consent.

Motives for creating viruses can include seeking profit; desire to send a political message, personal amusement, to demonstrate that vulnerability exists in software, for sabotage and denial of service.

Viruses often are classified based on the type of damage they do when infected. The major types are:

a. **Master Boot Record (MBR) Viruses:** Affects the boot sector of storage device and further infects when the storage is accessed.

b. **Stealth Viruses:** Stealth viruses hide themselves by tampering the operating system to fool antivirus software into thinking that everything is functioning normally.

c. **Polymorphic Viruses:** Polymorphic viruses are difficult to detect because they can modify themselves and change their identity thus able to hide themselves from antivirus software

d. **Macro Viruses:** Macro viruses are the most prevalent computer viruses and can easily infect many types of applications, such as Microsoft Excel and Word.

e. **Worms:** Worms are stand-alone viruses that are they are transmitted independently and executes themselves.

f. **Trojan Horse:** Malicious code hidden under legitimate programme, such as a game or simple utility. Trojans are primarily used by attackers to infect the system and then get control remotely to make that system work for them.

Logic Bomb/Time Bomb

Logic bombs are malicious code added to an existing application to be executed at a later date. These can be intentional or unintentional. For example Year 2000 problem was an unintentional logic bomb. Every time the infected application is run, the logic bomb checks the date to see whether it is time to run the bomb. If not, control is passed back to the main application and the logic bomb waits. If the date condition is correct, the rest of the logic bomb's code is executed and the result can be anything from a harmless message to a system crash.

6.3.12 Virus/Malicious Code protection mechanisms

Various countermeasures that can be deployed to protect against virus are:

a) **Anti-Virus:** Antivirus is most common protection from virus and is installed on most of laptops and desktops. Most of the antivirus software utilizes a method known as signature detection to identify potential virus infections on a system. Essentially, they maintain an extremely large database that contains the known characteristics (signatures) of all viruses. Depending upon the antivirus package and configuration settings, it can scan storage media periodically, check for any files that contain data matching those criteria. Antivirus tools have three types of controls –

- **Active monitor:** Monitors traffic and activity to check the viruses. Although most tools use signatures, few have developed heuristic scan abilities to look for possible malicious codes
- **Repair or quarantine:** These tools tries to remove the virus from file/mail or quarantines and reports.
- **Scheduled scan:** Users are prompted for scanning the storages to detect virus already present, that were not detected by active monitors. This happen when the new virus enters the system. (Zero day attack)

It is essential to ensure following controls:

- Virus signatures are updated
- Alerts from antivirus are reviewed for root cause
- Schedules scans are performed regularly

b) **Incident handling:** Incident Handling is an action plan for dealing with virus attack, intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. In case of virus incidents it is most essential to find out root cause to ensure that the incident does not recur.

c) **Training and Awareness programmes:** It is said that human beings are the weakest link in information security. Periodic training and awareness programmes need to be organized to ensure that employees and other 3rd party users are made aware of the risks arising out of improper use of organisation's information systems. These cover:

- Enforcing policy on use of removable devices
- Handling of mail attachments particularly from unknown senders
- Accessing internet
- Ensuring antivirus is updated and scheduled scan are performed (generally it is automated and centralised)

6.4 Current Trends in attacks

Most attacks and threats discussed above are being in use for a considerable time. Organisations being aware of their existence mostly ensure that controls are in place to prevent, detect and/or recover from these attacks. However attackers are always a step ahead. Attackers are now using other means to attack some of these are discussed below.

6.4.1 Exploiting application vulnerabilities

With use of internet based technologies and clouds organisations have hosted applications that can be accessed from internet and/or intranet. These applications might contain vulnerabilities if exploited can compromise the security of information. Attackers tried to exploit these vulnerabilities to launch the attacks like SQL Injection, Cross site scripting. OWASP (Open web application Security project) identifies top ten security threats every years. Threats identified in 2013 are listed below. (Source: www.owasp.org)

- **Injection (SQL Injection):** Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
- **Broken Authentication and Session Management:** Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

- **Cross-Site Scripting (XSS):** XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
- **Insecure Direct Object References:** A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorised data.
- **Security Misconfiguration:** Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
- **Sensitive Data Exposure:** Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
- **Missing Function Level Access Control:** Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorisation.
- **Cross-Site Request Forgery (CSRF):** A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
- **Using Components with Known Vulnerabilities:** Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defences and enable a range of possible attacks and impacts.
- **Invalidated Redirects and Forwards:** Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorised pages.

6.4.2 Advanced Persistent Threat (APT)

A sustained targeted attack on identified subject. Attacker tried to introduce malware to compromise the system. For this attacker uses possible social engineering methods. Once the system is compromise the malware resides in system. Since malware is specifically written antivirus may not be able to detect it. This malware is designed to send small bits of information from system to attacker without getting detected by network based controls like anomaly detection, traffic analysis etc. The attack continues for a longer duration till all required confidential information about organisation is received by the attacker.

6.5 Network Security Controls

This section examines controls available to ensure network security from the various threat identified listed earlier. The controls are listed under the following broad heads.

- Architecture
- Cryptography/Encryption
- Content Integrity
- Strong Authentication
- Remote Access Security
- Firewalls
- Intrusion Detection Systems
- Monitoring (Security Incident and Event Management (SIEM))

6.5.1 Architecture

The architecture or design of a network can have a significant effect on its security. Some of the major considerations are:

- **Segmentation / Zoning:** Segmentation / Zoning can limit the potential for harm in a network in two important ways. Segmentation reduces the number of threats, and it limits the amount of damage a single vulnerability can allow. A web server, authentication server, applications and database are residing on a single server or segment for facilitating electronic commerce transactions are a very insecure configuration. A more secure design will use multiple segments. Since the web server has to be exposed to the public, that server should not have other more sensitive, functions on it or residing on the same segment such as user authentication or access to the database. Separate segments and servers reduce the potential harm should any subsystem be compromised. (Please see figure 6.2 in next page).
- **Redundancy:** Another key architectural control is redundancy, allowing a function to be performed on more than one node. Instead of having a single web server; a better design would have two servers, using a “failover mode”. If one server is used and that server is down for some reason the whole application is not available. In failover mode, the servers communicate with each other periodically, each determining if the other is still active. If one fails, the other takes over processing for both of them. Although performance is cut approximately in half when a failure occurs, some minimum processing is being done which can be used to maintain critical functions.
- **Eliminate Single Points of Failure:** Good network architecture provides for its availability by eliminating single points of failure. This is true for all critical components including servers, network devices and communication channels in a network that will compromise its availability, if it fails.

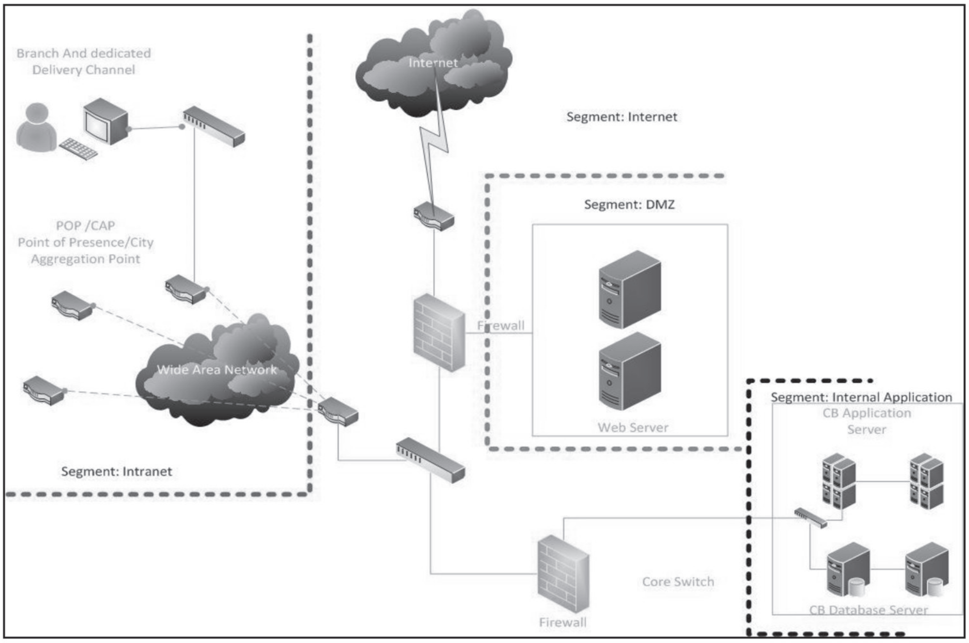


Figure 6.2: Segmented Architecture

6.5.2 Cryptography/Encryption

The technical details of cryptography have been dealt with in an earlier module. Only certain applications of cryptography that are relevant to Network security are discussed here.

Link Encryption

In link encryption, data are encrypted just before the system places them on the physical communications link, that is, encryption occurs at the Data Link layer in the OSI model. Correspondingly, decryption occurs at the Data Link layer of the receiving host. Link encryption protects the message in transit between two computers, but the message is in plaintext inside the hosts (above the data link layer). Headers added by the network layer (which includes addresses, routing information and protocol) and above are encrypted, along with the message/data. The message is, however, exposed at the Network layer and thus all intermediate nodes through which the message passes can read the message. This is because all routing and addressing is done at the Network layer. Link encryption is invisible to user and appropriate when the transmission line is the point of greatest vulnerability. Link encryption provides protection against traffic analysis.

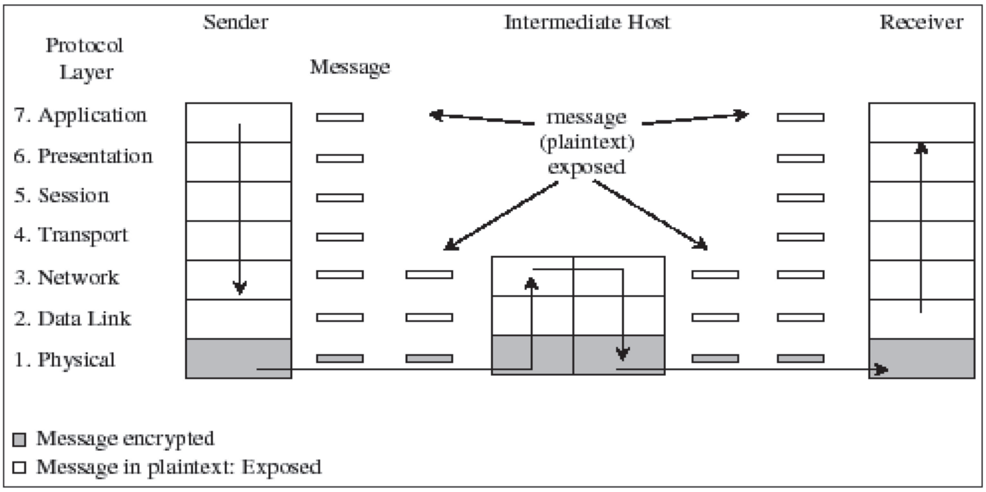
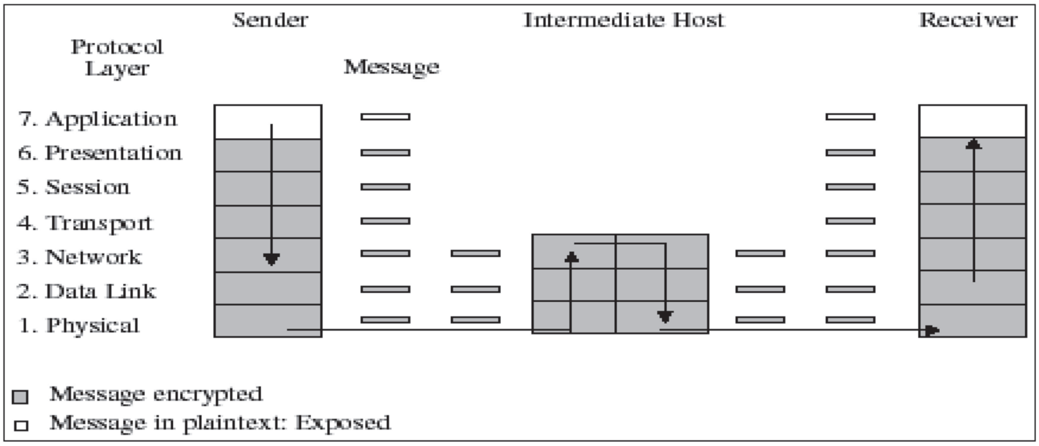


Figure 6.3: Link Encryption

End-to-End Encryption



End-to-end encryption provides security from one end of a transmission to the other. The encryption can be applied by a hardware device between the user and the host or the encryption can be done by software running on the host computer. In either case, the encryption is performed at the higher layers, usually application or presentation layer. When end-to-end encryption is used, messages, even when sent through several insecure intermediate hosts, are protected. This is because the data content remains encrypted at all the intermediate layers. However, since the headers below the transport is not encrypted (networks, data link, etc.) end-to-end does not provide protection against traffic analysis. Note that it is possible use both Link and End-to-end encryption at the same time. One does not preclude the other.

Figure 6.4: End-to-End Encryption

Table 6.1: Comparison of Link and End-to-End Encryption

Link Encryption	End-to-End Encryption
Security within hosts	
Data exposed in sending host	Data encrypted in sending host
Data exposed in intermediate nodes	Data encrypted in intermediate nodes
Role of user	
Applied by sending host	Applied by sending process
Invisible to user	User applies encryption
Host maintains encryption	User must find algorithm
One facility for all users	User selects encryption
Typically done in hardware	Either software or hardware implementation
All or no data encrypted	User chooses to encrypt or not, for each data item
Implementation concerns	
Requires one key per host pair	Requires one key per user pair
Provides node authentication	Provides user authentication

PKI and Certificates

A public key infrastructure (PKI) is a process created to enable users to implement public key (asymmetric) cryptography, usually in a large and distributed setting. PKI offers each user a set of services, related to identification and access control, as follows:

- Create certificates associating a user's identity with a (public) cryptographic key
- Issue certificates from its database
- Sign certificates, adding its credibility to the authenticity of the certificate
- Confirm (or deny) the validity of a certificate
- Revoke certificates for users who no longer are allowed access or whose private key has been exposed

PKI is a set of policies, procedures and products and not a standard. The policies define the rules under which the cryptographic systems should operate. In particular, the policies specify how to handle keys and valuable information and how to match level of control to level of risk. The procedures dictate how the keys should be generated, managed, and used. Finally, the products actually implement the policies, and they generate, store, and manage the keys. Entities, called certificate authorities, implement the PKI policy on certificates. The functions of a certificate authority can be done in-house or by a commercial service or a trusted third party. PKI may also involve a registration authority that acts as an interface between a user and a certificate authority. The registration authority captures and authenticates the identity of a user and then submits a certificate request to the appropriate certificate authority.

SSL Encryption

The SSL (Secure Sockets Layer) protocol was originally designed by Netscape to protect communication between a web browser and server. It is also known now as TLS, for transport layer security. SSL interfaces between applications (such as browsers) and the TCP/IP protocols to provide server authentication, optional client authentication, and an encrypted communications channel between client and server.

To create a SSL connection, the client requests an SSL session. The server responds with its public key certificate so that the client can determine the authenticity of the server. The client returns symmetric session key encrypted under the server's public key. The server decrypts the session key and then they switch to encrypted communication, using the shared session key.

IPSec

IETF (Internet Engineering Task Force) adopted IPSec, or the IP Security Protocol Suite. Designed to address spoofing, eavesdropping, and session hijacking, the IPSec protocol defines a standard means for handling encrypted data. IPSec is implemented at the IP layer, so it affects all layers above it, in particular TCP and UDP.

IPSec is similar to SSL, in that it supports authentication and confidentiality in a way that does not necessitate significant change either above it (in applications) or below it (in the TCP protocols). Like SSL, it was designed to be independent of specific cryptographic protocols and to allow the two communicating parties to agree on a mutually supported set of protocols.

Physical Header	IP Header	TCP Header	Data	Physical Trailer

Figure 6.5: Traditional Packets

Physical Header	IP Header	ESP Header (TCP Header + Data)	Physical Trailer

Figure 6.6: IPSec Packet

Signed Code

As already noted, it is possible for someone to place malicious active code on a web site to be downloaded by unsuspecting users. A partial solution to reduce this risk is to use signed code. A trustworthy third party appends a digital signature to a piece of code (or macro), supposedly connoting more trustworthy code. A signature structure in a PKI helps to validate the signature. A well-known manufacturer would be recognisable as a code signer.

Encrypted E-mail

An electronic mail message generally has no privacy at all. The service provider and any intermediate host can read not just the address but also everything in the message field. To protect the privacy of the message and routing information, we need encryption to protect the confidentiality and integrity of the message. The two popular approaches to key management are using a hierarchical, certificate based PKI solution for key exchange and using a flat, individual-lo-individual exchange method. The hierarchical method is called SMIME (Secure Multi-Purpose Mail Extensions) and is employed by many commercial mail programmes, such as Microsoft Exchange. The individual method is called PGP (Pretty Good Privacy) and is a commercial add-on.

6.5.3 Content Integrity

Content integrity is automatically implied when cryptographic systems are used. Most kinds of malicious threats are addressed by cryptographic systems very effectively. For non-malicious threats to integrity, the controls are Error Correcting codes and Message Digests (Cryptographic Checksums)

Error Correcting Codes

Error detection codes detect when an error has occurred, and error correction codes can actually correct errors without requiring retransmission of the original message. The error code is transmitted along with the original data, so the recipient can re-compute the error code and check whether the received result matches the expected value.

- **Parity Check:** The simplest error detection code is a parity check. An extra bit (the parity bit) is added to an existing group of data bits depending on their sum. With even parity the extra bit is 0 if the sum of the data bits is even and 1 if the sum is odd; that is, the parity bit is set so that the sum of all data bits plus the parity bit is even. Odd parity is the same except the sum is odd. Parity bits are useful only when the error is in a single bit (called single bit error).
- **Checksum and CRCs:** A checksum is a form of redundancy check that at its simplest, works by adding up the basic components of a message, usually the bits or bytes, and storing the resulting value. Later, anyone who has the authentic checksum can verify that the message was not corrupted by doing the same operation on the data, and checking the sum. A more sophisticated type of redundancy check is the cyclic redundancy checks (CRC) which considers not only the value of each bit/byte but also the order of the values. A cyclic redundancy check (CRC) uses a hash function used to produce a checksum which is a small integer from a large block of data, such as network traffic or computer files, in order to detect errors in transmission or duplication. CRCs are calculated before and after transmission or duplication, and compared to confirm that they are the same.
- **Other Codes:** Other kinds of error detection codes, such as hash codes and Hamming codes are used to detect burst errors (several errors occurring contiguously) and multiple bit errors (multiple errors among non-adjacent bits). Some of the more complex codes (like Hamming codes) can detect multiple-bit errors and may be able to pinpoint which bits have been changed, thus allowing the data to be corrected.

Message Digests (Cryptographic Checksums)

Checksums and CRCs are useful in detecting accidental modification such as corruption to stored data or errors in a communication channel. However, they provide no security against malicious agents, as their simple mathematical structure makes them trivial to circumvent. To protect against malicious changes cryptographic checksum are used. A cryptographic checksum is created by performing a complicated series of mathematical operations (the cryptographic algorithm) that translates the data in the file into a fixed string of digits called a hash value, which is then used as a checksum. Without knowing which cryptographic algorithm was used to create the hash value, it is highly unlikely that an unauthorised person would be able to change data without inadvertently changing the corresponding checksum.

A cryptographic hash function must ensure that the following is computationally infeasible:

- Determining the content of a message from its Cryptographic Checksums
- Finding "collisions", wherein two different messages have the same Cryptographic Checksums.

Cryptographic checksums are also known as message digests, message authentication codes, integrity check-values, modification detection codes, or message integrity codes.

6.5.4 Strong Authentication

A security policy specifies who which individuals, groups, subjects can access which resources and objects. Crucial to that policy is authentication: knowing and being assured of the accuracy of identities. Organisation must adopt strong authentication methods appropriate for use in networks like one-time passwords, Challenge Response systems and Kerberos, discussed in previous chapter.

6.5.5 Remote Access Security

Remote access technologies can be defined as those data networking technologies that are focused on providing the remote user with access into a network, while striving to maintain the principal tenets of Confidentiality, Availability, and Integrity. There are many obvious advantages to employing secure remote network access, such as the following:

- Reducing networking costs by using the Internet to replace expensive dedicated network lines
- Providing employees with flexible work styles such as telecommuting
- Building more efficient ties with customers, suppliers, and employees

Virtual Private Networking (VPN)

A virtual private network (VPN) is created by building a secure communications link between two nodes by emulating the properties of a point-to-point private link. A VPN can be used to facilitate secure remote access into a network, securely connect two networks together, or create a secure data tunnel within a network. Encryption coupled with access controls (including firewalls) can provide users with the same level of privacy that can be provided on a private network, even when the communication traverses a part of the public network. For more details, refer the previous module.

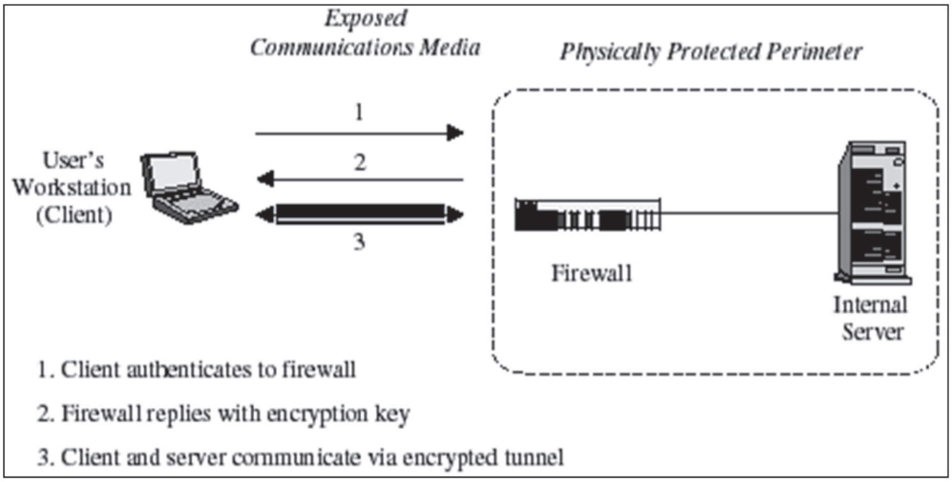

Exposed
Communications Media
Physically Protected Perimeter
1
2
3
User's
Workstation
(Client)
Firewall
Internal
Server
1. Client authenticates to firewall
2. Firewall replies with encryption key
3. Client and server communicate via encrypted tunnel

Figure 6.7: Secure VPN

Dial back procedures

In a networked computing environment, user may often require access to the systems resources from remote locations. Dial-back systems are a control to ensure that access is made only from authorised lines or locations. When a user dials into the server and identifies itself, the server hangs up and calls the user at a pre-determined telephone number and then enables the user to access the resources based on password authentication. A weakness in this procedure is call-forwarding. An unauthorised person could enable calls to a pre-determined number to be forwarded to the number designated by him, thus enabling him to gain unauthorised access to the resources.

Other controls

To minimise the risk of unauthorised dial-in access, remote users should never store their passwords in plain text login scripts on notebooks and laptops.

Authentication Servers

In widely spread out networked systems, the problem of user management and enabling authorised access is crucial since users are spread over a wide geographical areas including telecommuting. In such cases all access control is transferred to a centralised or decentralised access authentication mechanism. Two of the popular applications of remote authentication mechanisms depending on centralised/decentralised access authentication implementations are TACACS (Terminal Access Controller Access Control System) and RADIUS (Remote Authentication Dial in User Service). Some of the features of such systems are:

- Enable secure remote access
- Facilitates centralised user management
- Facilitates centralised access monitoring and control

- Changes to user access rights made easy
- Provides event logging and extended audit trails

6.5.6 Firewalls

The technical details of firewalls, their types and configurations have been dealt with in the first module. Only certain specialised applications of firewalls for network security are dealt with here.

Intranet

An intranet is a network that employs the same types of services, applications, and protocols present in an Internet implementation, without involving external connectivity. For example, an enterprise network employing the TCP/IP protocol suite, along with HTTP for information dissemination would be considered an Intranet. Most organisations currently employ some type of intranet, although they may not refer to the network as such. Within the internal network (intranet), many smaller intranets can be created by the use of internal firewalls. As an example, an organisation may protect its personnel network with an internal firewall, and the resultant protected network may be referred to as the personnel intranet. Since intranets utilize the same protocols and application services present on the Internet, many of the security issues inherent in Internet implementations are also present in intranet implementations. Therefore, intranets are typically implemented behind firewall environments.

Extranets

An extranet is usually a business-to-business intranet; that is, two intranets are joined via the Internet. The extranet allows limited, controlled access to remote users via some form of authentication and encryption such as provided by a VPN. Extranets share nearly all of the characteristics of intranets, except that extranets are designed to exist outside a firewall environment. By definition, the purpose of an extranet is to provide access to potentially sensitive information to specific remote users or organisations, but at the same time denying access to general external users and systems. Extranets employ TCP/IP protocols, along with the same standard applications and services. Many organisations and agencies currently employ extranets to communicate with clients and customers. Within an extranet, options are available to enforce varying degrees of authentication, logging, and encryption.

Securing a Firewall

Firewall platforms should be implemented on systems containing operating system builds that have been stripped down and hardened for security applications. Firewalls should never be placed on systems built with all possible installation options. Firewall operating system builds should be based upon minimal feature sets. All unnecessary operating system features should be removed from the build prior to firewall implementation. All appropriate operating system patches should be applied before any installation of firewall components.

The operating system build should not rely strictly on modifications made by the firewall installation process. Firewall installation programmes rely on a lowest common denominator approach; extraneous software packages or modules might not be removed or disabled during the installation process.

The hardening procedure used during installation should be tailored to the specific operating system undergoing hardening. Some often-overlooked issues include the following:

- Any unused networking protocols should be removed from the firewall operating system build. Unused networking protocols can potentially be used to bypass or damage the firewall environment. Finally, disabling unused protocols ensures that attacks on the firewall utilizing protocol encapsulation techniques will not be effective.
- Any unused network services or applications should be removed or disabled. Unused applications are often used to attack firewalls because many administrators neglect to implement default-restrictive firewall access controls. In addition, unused network services and applications are likely to run using default configurations, which are usually much less secure than production-ready application or service configurations.
- Any unused user or system accounts should be removed or disabled. This particular issue is operating system specific, since all operating systems vary in terms of which accounts are present by default as well as how accounts can be removed or disabled.
- Applying all relevant operating system patches is also critical. Since patches and hot fixes are normally released to address security-related issues, they should be integrated into the firewall build process. Patches should always be tested on a non-production system prior to rollout to any production systems.
- Unused physical network interfaces should be disabled or removed from the server chassis.

6.5.7 Intrusion Detection Systems

After the perimeter controls, firewall, and authentication and access controls block certain actions, some users are admitted to use a computing system. Most of these controls are preventive, that is, they prevent known undesirable things from happening. Many studies, however, have shown that most computer security incidents are caused by insiders, people who would not be blocked by a firewall. And insiders require access with significant privileges to do their daily jobs.

Intrusion detection systems complement these preventive controls as the next line of defence. An intrusion detection system (IDS) is a device, usually another separate computer, which monitors activity to identify malicious or suspicious events. An IDS is a sensor that raises an alarm if specific things occur. The alarm can range from writing an entry in an audit log, to something significant, such as paging the system security administrator. An IDS receives inputs from sensors. It saves those inputs, analyses them, and takes some controlling action.

The functions performed by IDS are:

- Monitoring users and system activity
- Auditing system configuration for vulnerabilities and mis-configurations
- Assessing the integrity of critical system and data files
- Recognising known attack patterns in system activity
- Identifying abnormal activity through statistical analysis
- Managing audit trails and highlighting user violation of policy or normal activity
- Correcting system configuration errors

- Installing and operating traps to record information about intruders
- Special considerations in audit of remote access and network security

Many intrusion detection systems are also capable of interacting with firewalls in order to bring a reactive element to the provision of network security services. Firewalls that interact with intrusion detection systems are capable of responding to perceived remote threats automatically, without the delays associated with a human response. For example, if an intrusion detection system detects a denial of service attack in progress, it can instruct certain firewalls to automatically block the source of the attack (although, false positives responses can occur).

The two general types of intrusion detection systems are signature based and heuristic. Signature-based intrusion detection systems perform simple pattern-matching and report situations that match a pattern corresponding to a known attack type. Heuristic intrusion detection systems, also known as anomaly based, build a model of acceptable behaviour and flag exceptions to that model; for the future, the administrator can mark a flagged behaviour as acceptable so that the heuristic IDS will now treat that previously unclassified behaviour as acceptable.

Intrusion detection devices can be network based or host based. A network-based IDS is a stand-alone device attached to the network to monitor traffic throughout that network; a host-based IDS runs on a single workstation or client or host, to protect that one host. For more details, please see the previous module.

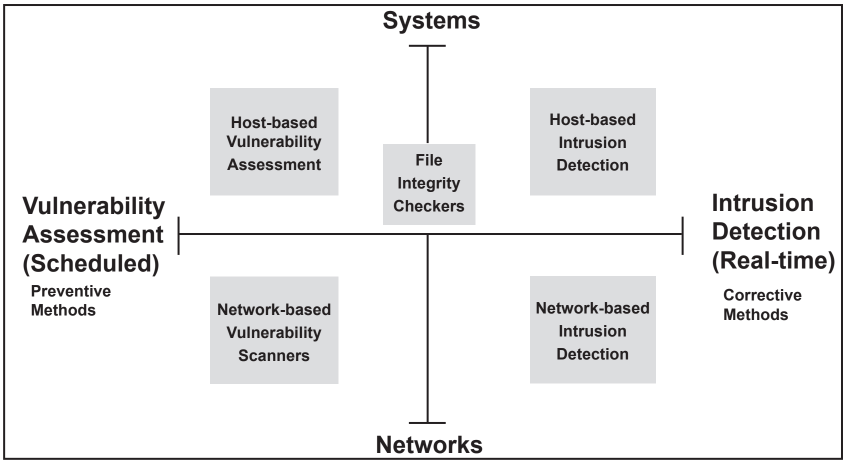

Systems
Host-based Vulnerability Assessment
File Integrity Checkers
Host-based Intrusion Detection
Vulnerability Assessment (Scheduled)
Preventive Methods
Intrusion Detection (Real-time)
Corrective Methods
Network-based Vulnerability Scanners
Network-based Intrusion Detection
Networks

Figure 6.8: Intrusion Detection System

6.6 Monitoring Controls

Most controls implemented for network generates lot of logs related to activities as per rule set. Monitoring and reviewing these logs is a mammoth task and need lot of efforts and resources. There are various tools available in market that helps organisations in collecting these logs, co-relating them based on possible use cases and generate alerts for important logs. This way the efforts can be minimised, however cannot be eliminated. Also resources required to manage these tools are specially trained and skilled.

These tools are known as Security Incident and Event Management (SIEM) tools. Organisations use these tools and establish a security operations centre (SOC) to monitor these logs, analyse alerts and record incidents and events to be responded. Broad Objectives of SOC are:

- Detect attacks and malware
- Enhance incident response capability
- Detect Advanced persistent threats
- Compliance requirements

A typical SOC is connected with other systems as shown in Figure 6.9.

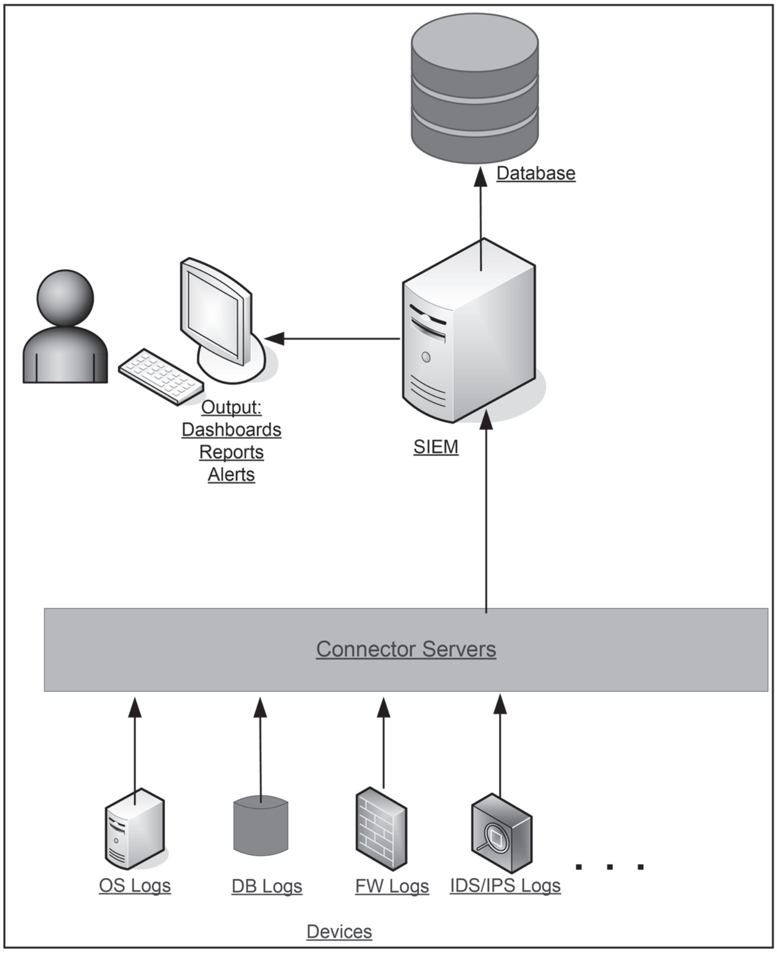


Figure 6.9: Security Operations Centre

Establishing SOC requires huge cost and resources and small organisations may prefre to outsource such services to vendor.

6.7 Endpoint security

In network security, endpoint security refers to a methodology of protecting the corporate network when accessed via remote devices such as laptops or other wireless and mobile devices. Each device with a remote connection to the network creates a potential entry point for security threats. Endpoint security is designed to secure each such access from the endpoint (device) to the network resources.

Usually, endpoint security is a security system that consists of security software, located on a centrally managed and accessible server or gateway within the network, in addition to client software being installed on each of the endpoints (or devices). The server authenticates logins from the endpoints and also updates the device software when needed. As an endpoint wants to make an access to the network, the server software authenticates the device (i.e. the end point) and checks whether it conforms to the security policy of the organisation before allowing the access. While endpoint security software differs by vendor, you can expect most software offerings to provide antivirus, antispyware, personal firewall and also a host intrusion prevention system.

Endpoint security is becoming a more common IT security function and concern as more employees bring consumer mobile devices to work and companies allow its mobile workforce to use these devices on the corporate network.

6.8 Wireless Security threats and Risk Mitigation

A wireless network is a type of computer network that uses wireless data connections for connecting network nodes. It is a method by which enterprise (office), homes, etc. avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.

Wireless networking presents many advantages like network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile. For example, because communication takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can intercept and read it, thereby compromising confidentiality.

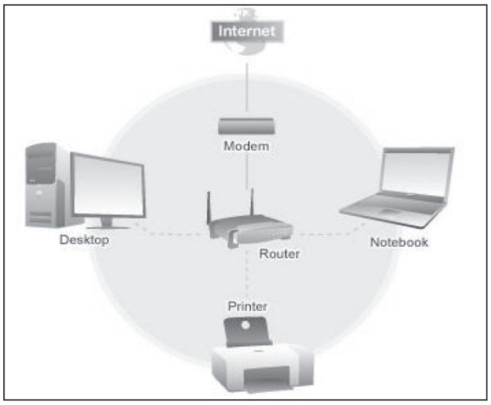


Figure 6.10: Typical wireless network

Wireless network has numerous vulnerabilities such as:

- **Ad-hoc networks:** *Ad-hoc* networks can pose a security threat. *Ad-hoc* networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them.
- **Non-traditional networks:** Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured. These non-traditional networks are commonly overlooked by IT personnel who have narrowly focused on laptops and access points.
- **MAC spoofing:** MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address is hard-coded on a network interface card (NIC) and cannot be changed. However, there are tools which can make an operating system believe that the NIC has a MAC address different than it's real MAC address.
- **Man-in-the-middle attacks:** A man-in-the-middle attack is an attack in which an attacker secretly intercepts the electronic messages going between the sender and the receiver and then capture, insert and modify messages during message transmission
- **Accidental association:** Unauthorised access to organisation's wireless and wired networks can come from a number of different methods and intents. One of these methods is referred to as "accidental association". When a user turns on a computer and it latches on to a wireless access point from a neighbouring organisation's overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary organisation information is exposed and now there could exist a link from one organisation to the other. This is especially true if the laptop is also hooked to a wired network.
- **Denial of service:** It is an attempt to make a machine not available to its intended user.

Wireless network provides numerous opportunities to increase productivity and manage costs. Although it is impossible to totally eliminate all risks associated with wireless networking, it is possible to achieve a reasonable level of security by adopting a systematic approach to assessing and managing risk. Most common controls which are implemented in wireless environment are:

- **Encryption:** The best method for protecting the confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic.
- **Signal-Hiding Techniques:** In order to intercept wireless transmissions, attackers first need to identify and locate wireless networks. There are, however, a number of steps that an organisation can take to make it more difficult to locate their wireless access points. The easiest options include: Turning off the service set identifier (SSID) broadcasting by wireless access points and reducing signal strength to the lowest level that still provides requisite coverage. More effective, but also more costly methods for reducing or hiding signals include: using directional antennas to constrain signal emanations within desired areas of coverage or using signal emanation-shielding techniques, also referred to as TEMPEST to block emanation of wireless signals.
- **Anti-virus and anti-spyware software:** Computers on a wireless network need the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the "off" mode, turn it on.

- **Default passwords:** Wireless routers generally come with standard default password that allows you to set up and operate the router. These default passwords are also available on the web. So change the router password immediately after its installation.
- **MAC address:** Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses access to the network.

6.9 Voice-over IP

Voice over Internet Protocol (VoIP) is a methodology for delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB) and broadband telephony.

The term Internet telephony specifically refers to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN). The steps and principals involved in originating VoIP telephone calls are similar to traditional digital telephony, and involve signalling, channel setup, digitisation of the analog voice signals, and encoding. Instead of being transmitted over a circuit-switched network, however, the digital information is packetised and transmission occurs as Internet Protocol (IP) packets over a packet-switched network. VoIP is available on many smartphones, personal computers, and on Internet access devices. Calls and SMS text messages may be sent over 3G or Wi-Fi.

6.9.1 Security Threats to VoIP

VoIP systems rely on a data network, which means security weaknesses and the types of attacks associated with any data network are possible. For example, in a conventional telephone system, physical access to the telephone lines or a compromise of the office private branch exchange (PBX) is required for in order to conduct activities such as wire-tapping. But for VoIP, voice is converted into IP packets that may travel through many network access points. Therefore the data is exposed to many more possible points of attack that could be used for interception by intruders. In fact, all the security risks associated with IP, such as computer viruses, Denial of Service and man in the middle attacks, are also dangerous to VoIP systems. Most of the VoIP traffic over the Internet is not encrypted, so this traffic is exposed to the hackers. Hackers can intercept the communication or shut down the voice services by flooding servers (supporting VoIP) with bogus traffic.

6.9.2 VoIP Security

Encryption: Encryption is a means of preserving the confidentiality of transmitted signals.

a. **Physical security:** Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to perform traffic analysis and derive call information from encrypted messages. Therefore, adequate physical security should be in place to restrict access to key VoIP network components.

b. **Anti-virus and firewalls:** Computers which use software for VoIP connections should be protected with a personal firewall, along with anti-virus and anti-malicious code software that are up to date with the latest virus signature and/or malicious code definitions. This provides basic protection against attacks on the data segment that could be transferred to the voice segment.

c. **Segregation of Voice and Data segments:** IP-based telephony provides a platform for telephone calls over an existing IP data network. However, in order to maintain quality of service (QoS), scalability, manageability, and security, voice and data should be separated using different logical networks as far as possible. Segmenting IP voice from a traditional IP data network greatly enhances the mitigation of VoIP attacks.

6.10 Penetration Testing

Penetration Testing is used by organisations to evaluate the effectiveness of information security implementation. As its name implies, penetration testing is a series of activities undertaken to identify and exploit security vulnerabilities. The idea is to find out how easy or difficult it might be for someone to "penetrate" an organisation's security controls or to gain unauthorised access to its information and information systems.

A penetration test is performed by team of experts. This team simulates attack using similar tools and techniques used by hackers. Penetration test cannot be expected to identify all possible security vulnerabilities because penetration testing is conducted at a point in time. New technology, new hacker tools and changes to an organisation's information system can create exposures not anticipated during the penetration testing. Hence organisations perform these tests periodically.

Penetration Testing Scope

The scope of a penetration testing is to determine whether an organisation's security vulnerabilities can be exploited and its systems compromised. Conducting such a test involves gathering information about an organisation's information systems and information security and then using this information to attempt to identify and exploit known or potential security vulnerabilities. Evidence to support the penetration testing team's ability to exploit security vulnerabilities can vary from gathering "computer screen shots" or copying sensitive information or files to being able to create new user accounts on the system or being able to create and/ or delete particular files on the organisation's servers. Penetration testing can have a number of secondary objectives, including testing the security incident identification and response capability of the organisation, testing employee security awareness or testing users' compliance with security policies.

Penetration Testing Strategies

Various strategies for penetration testing, based on specific objectives to be achieved, include:

- **External vs. internal testing:** External testing refers to attacks on the organisation's network perimeter using procedures performed from outside the organisation's systems as they are visible to hacker. This can be a **Blind test** where testing expert has been provided with limited information.
- **Internal testing :** Is performed from within the organisation's technology environment. The focus is to understand what could happen if the network perimeter were successfully penetrated or what an authorised user could do to penetrate specific information resources within the organisation's network.

- **Targeted testing:** (often referred to as the "lights-turned-on" approach) involves both the organisation's IT team and the penetration testing team being aware of the testing activities and being provided information concerning the target and the network design. A targeted testing approach may be more efficient and cost-effective when the objective of the test is focused more on the technical setting, or on the design of the network, than on the organisation's incident response and other operational procedures. A targeted test typically takes less time and effort to complete than blind testing, but may not provide as complete a picture security vulnerabilities and response capabilities of the organisation.

6.10.1 Types of Penetration Testing

In addition to the penetration testing strategies to be used, consideration should be given to the types of testing the testing team is to carry out. These could include:

- **Application security testing:** Many organisations offer access to core business functionality through web-based applications. This type of access introduces new security vulnerabilities, because even with a firewall and other monitoring systems, security can be compromised, since traffic must be allowed to pass through the firewall. The objective of application security testing is to evaluate the controls over the application and its process flow. Areas of evaluation may include the application's usage of encryption to protect the confidentiality and integrity of information, how users are authenticated, integrity of the Internet user's session with the host application, and use of cookies – a block of data stored on a customer's computer that is used by the web server application.
- **Denial of Service (DoS) testing:** The goal of DoS testing is to evaluate the system's susceptibility to attacks that will render it inoperable so that it will "deny service," that is, drop or deny legitimate access attempts. Decisions regarding the extent of Denial of Service testing to be incorporated into a penetration testing exercise will depend on the relative importance of ongoing, continued availability of the information systems and related processing activities.
- **War Dialling:** War dialling is a technique for systematically calling a range of telephone numbers in an attempt to identify modems, remote access devices and maintenance connections of computers that may exist on an organisation's network. Well-meaning users can inadvertently expose the organisation to significant vulnerability by connecting a modem to the organisation's information systems. Once a modem or other access device has been identified, analysis and exploitation techniques are performed to assess whether this connection can be used to penetrate the organisation's information systems network.
- **Wireless network penetration testing:** The introduction of wireless networks, whether through formal, approved network configuration management or the inadvertent actions of well-meaning users, introduce additional security exposures. Sometimes referred to as "war-driving," hackers have become proficient in identifying wireless networks simply by "driving" or walking around office buildings with their wireless network equipment. The goal of wireless network testing is to identify security gaps or flaws in the design, implementation or operation of the organisation's wireless network.
- **Social Engineering:** Often used in conjunction with blind and double blind testing, this refers to techniques using social interaction, typically with the organisation's employees, suppliers and contractors, to gather information and penetrate the organisation's systems.

Such techniques could include:

- Posing as a representative of the IT department's help desk and asking users to divulge their user account and password information;
- Posing as an employee and gaining physical access to restricted areas that may house sensitive information;
- Intercepting mail, courier packages or even trash to search for sensitive information on printed materials.

Social engineering activities can test a less technical, but equally important, security component: the ability of the organisation's people to contribute to, or prevent, unauthorised access to information and information systems.

6.10.2 Risks associated with Penetration Testing

While management sponsors the testing activities, those activities do, in themselves, represent some level of risk. Some of the key risks include the following:

- The penetration test team may fail to identify significant vulnerabilities;
- Misunderstandings and miscommunications may result in the test objectives not being achieved;
- Testing activities may inadvertently trigger events or responses that may not have been anticipated or planned for (such as notifying law enforcement authorities);
- Sensitive security information may be disclosed, increasing the risk of the organisation being vulnerable to external attacks.

Generally penetration testing is performed by external experts, hence it is necessary to enforce non-disclosure agreement and also define content of report, since it will contain the vulnerabilities within the system.

Table 6.2: Network Vulnerabilities and Controls

Target	Vulnerability	Control
Precursors to attack	Port scan	Firewall Intrusion detection system Running as few services as possible Services that reply with only what is necessary
	Social engineering	Education, user awareness Policies and procedures Systems in which two people must agree to perform certain security-critical functions
	Reconnaissance	Firewall Hardened" (self-defensive) operating system and applications Intrusion detection system

Target	Vulnerability	Control
	OS and application fingerprinting	Firewall "Hardened" (self-defensive) applications Programmes that reply with only what is necessary Intrusion detection system
Authentication failures	Impersonation	Strong, one-time authentication
	Guessing	Strong, one-time authentication Education, user awareness
	Eavesdropping	Strong, one-time authentication Encrypted authentication channel
	Spoofing	Strong, one-time authentication
	Session hijacking	Strong, one-time authentication Encrypted authentication channel Virtual private network
	Man-in-the-middle attack	Strong, one-time authentication Virtual private network Protocol analysis
Programming flaws	Buffer overflow	Programming controls Intrusion detection system Controlled execution environment Personal firewall
	Addressing errors	Programming controls Intrusion detection system Controlled execution environment Personal firewall Two-way authentication
	Parameter modification, time-of-check to time-of-use errors	Programming controls Intrusion detection system Controlled execution environment Personal firewall Two-way authentication
	Server-side include	Programming controls Personal firewall Controlled execution environment Intrusion detection system
	Cookie	Firewall Intrusion detection system Controlled execution environment Personal firewall

Target	Vulnerability	Control
	Malicious active code: JavaScript, ActiveX	Intrusion detection system Controlled execution environment Signed code
	Malicious code: virus, worm, Trojan Horse	Intrusion detection system Signed code Controlled execution environment Intrusion detection system
	Malicious typed code	Signed code Intrusion detection system Controlled execution environment
Confidentiality	Protocol flaw	Programming controls Controlled execution environment
	Eavesdropping	Encryption
	Passive wiretap	Encryption
	Mis-delivery	Encryption
	Exposure within the network	End-to-end encryption
	Traffic flow analysis	Encryption Traffic padding Onion routing
	Cookie	Firewall Intrusion detection system Controlled execution environment
Integrity	Protocol flaw	Firewall Controlled execution environment Intrusion detection system Protocol analysis Audit
	Active wiretap	Encryption Error detection code Audit
	Impersonation	Firewall Strong, one-time authentication Encryption Error detection code Audit

Target	Vulnerability	Control
	Falsification of message	Firewall Encryption Strong authentication Error detection code Audit
	Noise	Error detection code
	Web site defacement	Error detection code Intrusion detection system Controlled execution environment Hardened host Honey pot Audit
	DNS attack	Firewall Intrusion detection system Strong authentication for DNS changes Audit
Availability	Protocol flaw	Firewall Redundant architecture
	Transmission or component failure	Architecture
	Connection flooding, e.g., echo-charge, ping of death, smurf, syn flood	Firewall Intrusion detection system ACL on border router Honey pot
	DNS attack	Firewall Intrusion detection system ACL on border router Honey pot
	Traffic redirection	Encryption Audit
	Distributed denial of service	Firewall Intrusion detection system ACL on border router Honey pot

The layers of security controls on the network are depicted in the following table.

Table 6.3: Layers of security controls on network

Security Level	Applicable Security/Control measures
Perimeter	Firewall Network-based anti-virus VPN encryption
Network	Intrusion detection /prevention system (IDS/IPS) Vulnerability management system Network access control Access control /user authentication
Host	Host IDS and Host vulnerability assessment (VA) Network access control Anti-virus Access control/user authentication
Application	Application shield Access control/user authentication Input validation
Data	Encryption Access control/user authentication

6.11 Auditing Network Security

Auditing networked computing environments presents significant complexities. Networking enables several virtual machines to operate together using a limited set of systems resources, irrespective of the barriers of geographic location of the user and systems infrastructure. For example, a customer can now access his bank account from anywhere in the world. This means that logical paths open up enabling access through insecure networks and diverse computing infrastructures. Audit of network security requires the auditor to take special considerations into account and plan accordingly to achieve his audit objectives. The considerations while auditing network security are:

- Locating logical access paths by reviewing network diagrams
- Identifying network topologies, virtual paths spanning across LANs, WANs and the open networks such as shared networks and the Internet.
- Recognising logical access threats, risks and exposures in the networked environment.
- Identifying and controlling over access paths used for distributed processing and distributed databases.
- Evaluating network management and change control in respect of technical components such as modems, switches, routers, firewalls, VPNs, network management and access control software, encryption, protocols, middleware controls and Internet security.
- Identifying information resource owners can be quite complex since in a distributed computing environment, an application process can span several systems and networks, including those outside the organisation’s control.

- Evaluating logical network security policies and practices.
- Evaluating effectiveness of logical access security with respect to network security components such as:
- Firewalls and filtering routers – architecture, configuration setting as per firewall security policy, port services, anti-virus configuration, reporting and management controls
- Intrusion detection systems – architecture, configuration, interface with other security applications, reporting and management controls
- Virtual private networks – architecture, devices, protocol, encryption process integration with firewall security, change management
- Security protocols – selection of appropriate protocol, seamless security integration of protocols between devices running different protocols
- Encryption – selection of appropriate encryption methods to various application processes
- Middleware controls – middleware design and access control with respect to identification, authentication and authorisation, management of components and middleware change management.
- Network event logging and monitoring

Type of System		Intrusion Detection				Vulnerability		
System Control Features		**Monitoring**				**Assessment**		
Controls **D-Detective** **P-Preventive** **C-Corrective** **S-Support**		Application Based	Host Based	Target Based	Network Based	Host Based	Network Based	Password Assessment
Confidentiality	Unauthorised access to files and system resources		D			P	P	P
	Modification to files		D	D		P	P	P
	Violation of enterprise system access polices	D	D			P	P	
	Violation of security policies	D	D	D	D	P	P	
	Weak or non-existent passwords	D	D			D		D
Integrity	Placement of Trojan Horse or malicious software		D	D		P	P	
	Presence of Trojan Horse or malicious software			D				

	Attack Against network services				D		P	
	Script based attacks	D			D	P		
Availability	Denial of Services Attacks				D		P	
	Failure or Mis-configuration of firewalls	D			D	P	P	
	Attacks Happening Over Encrypted Links	D	D					
	Unusual activity or variation from normal data pattern		D		D			
Other	Errors in Network configuration		D			DPC	DPC	
	Liability Exposure associated with attacker using own resources to attack others	P	P	P	P	P	P	P
	Post incident damage assessment	S	S	S	S	S	S	S

6.12 Summary

Networks are veins of market place. Organisations cannot imagine implementing IT without networks. Networks have added most important attribute to business performance that is efficiency. However it is not without risks. This has helps organisations in expanding their business empire and attackers in remaining unanimous. Most security breaches today are due to availability of networks. And therefore it is most essential for organisations to protect their networks in order ensure reasonable security has been implemented. IS auditor also must focus on the network security. Although sometimes it may not be in scope, but considering the architecture auditors cannot perform any IS audit without evaluating network controls. For example if the scope of audit is application control audit, auditor have consider network since the application is accessed by users over networks and sometimes using internet.

As technology is updating its capabilities, so are attackers and they are trying to use more and more innovative methods to attack organisations. IS auditors must be aware of trends in new technology as well as current threat scenarios.

6.13 Questions

1. Which of the following is a method used to gather information about the communication network?

   A. Reconnaissance

   B. Brute force

   C. Eavesdropping

   D. Wiretapping

2. Message digest helps organisation in getting assurance on:
   A. Communication delivery
   B. Data availability
   C. Data integrity
   D. Data confidentiality

3. While auditing organisation's network which of the following control IS auditor must verify first?
   A. Encrypted communication
   B. Network zoning
   C. Firewall configuration
   D. Penetration test report

4. Cryptographic checksum is a network control that:
   A. Adds a parity bit after adding the data bits.
   B. Translates data in a file into a hash value.
   C. Transmits the data after encryption.
   D. Translates the data into a parity checksum combination.

5. Primary function of Security operations centre (SOC) is to:
   A. Define baseline
   B. Configure firewall
   C. Monitor logs
   D. Implement Antivirus

6. The intrusion detection monitoring on a host for data integrity attack by malicious software is a:
   A. Technical control
   B. Corrective control
   C. Detective Control
   D. Preventive Control

7. Which of the following is most important while performing penetration testing?
   A. Maintain secrecy about testing.
   B. Get consent from affected stakeholders.
   C. Report to be provided to all users.
   D. Perform test after office hours.

8. Most web based application attacks can be prevented by:
   A. Input validation
   B. Encryption

C. Penetration test

D. Access controls

9. Social engineering attacks can best be prevented by:

A. Intrusion detection system

B. Strong access controls

C. Two factor authentication

D. Awareness training

10. Which of the following is a type of malware that can be unnoticed?

A. Virus

B. Logic bomb

C. Trojan

D. Worm

6.14 Answers and Explanations

1. A. Other methods are active attacks on network after getting information about networks.
2. C. Message digest is a hash function that helps in confirming integrity of data communicated over network.
3. B. Network segmentation or zoning is first control to implement network security. Other controls depends upon segmentation.
4. B. Checksum is a type of hash that is used to check integrity of data after communication. It is different that parity bit that adds an extra bit for each byte and word.
5. C. Primary function of SOC is to collect and monitor logs based on identified rules. It also defines correlation between various logs and identifies possible incidents which are communicated to respective asset owners. A is role of security manager, B and D are role of network team.
6. C. Intrusion detection detects the possible intrusion attempt. It does not prevent or corrects it. It is a control implemented using technology.
7. B. It is most essential to get consent from affected asset owners for before performing test, so that they can ensure that operations are not affected. Maintaining secrecy shall depend upon type of test. Report must be kept confidential and accessed only by select few. Test generally is performed when it will have least impact, but is not most important.
8. A. Most web application attacks like SQL injection can be prevented by validating input which can reject the attackers input that can exploit vulnerability. Encryption may or may not prevent an attack. Penetration test shall provide input on vulnerability that must be closed. Access controls may prevent some attacks.
9. D. Social engineering attack is attack on human and hence no technology can prevent it. It is best prevented by awareness training.
10. B. Logic bomb cannot be identified by any malware.

6.15 References

a. Publication:

Security in Computing, 3rd Edition, By Charles P. Pfleeger, Shari Lawrence Pfleeger Published Dec. 2, 2002 by Prentice Hall.

b. Websites

1) http://compnetworking.about.com/
2) http://theirm.org/
3) http://www.cert.org/
4) http://www.isaca.org/
5) http://www.iso.org/iso/home/standards/iso31000.htm
6) http://www.webopedia.com
7) https://na.theiia.org/Pages/IIAHome.aspx
8) https://www.dataprotection.ie/
9) www.ehow.com
10) www.en.wikipedia.org
11) www.firesafetyinstitute.org
12) www.resources.infosecinstitute.com/access-control-models-and-methods
13) www.technet.microsoft.com/en-us
14) www.owasp.org

SECTION 2 : APPENDIX

This section contains few checklist that might be useful for IS auditors while performing audit of different areas discussed in this module. Please note that contents of this section are for information and may not be complete in all respects. Auditors must pick and choose the different sections from these checklist while conducting audit and modify suitably as per the requirements and scope of audit.

1. Audit Checklist: Risk Management Process

Below are some of the suggested criteria and procedures for conducting an audit of risk management. The auditor's primary role is to ascertain whether the methods and procedures used were appropriate and conform to the policies and guidelines which make up the organisation's approach to risk management. The auditor's secondary role is to ensure that any identified deficiencies are dealt with and that follow-ups are made.

Sl. No.	Section	Control Objective	Audit Procedure
1	Risk Management framework	Organisation must have a risk management policy and framework that guides users in risk identification and assessment	Review Risk policies for common terminology, Risk response options and definition of risk and control owners Understand risk management process and framework. Interview managers that they understand the terminology, process and framework. Review risk register and its updating process Interview senior management to understand risk appetite and risk tolerance levels
2	Risk Identification	Management understands the risk identification concept and has identified key risks	Check whether all managers are aware of the key risks to the organisation and/or their function Assess the depth of the manager's understanding of the risk identification process based on his or her awareness Verify that managers have assessed the key risks to the organisation Assess the completeness and accuracy of the risk assessment
3	Risk Mitigation	Management has performed valid risk assessments.	Verify that management has documented risk assessments for each of the significant risks identified

Sl. No.	Section	Control Objective	Audit Procedure
		Management has selected and implemented cost-effective risk control measures.	Verify that management has developed a series of risk-minimisation, cost-effective options.
		As a result of implementing control measures, the overall risk to the organisation has declined.	Assess whether the control measures introduced have managed the threat from the threats, as intended
4	Risk Monitoring	Investigate incidents, changes, acquisitions, projects and verify that the management has reviewed risk associated with root cause and risk register is updated.	Review the root cause of incident and ensure updating of risk register Review changes and acquisitions and their linkage to risk registers during assessment of impact due to change Review project risk management process
5	Risk register	Review risk register to contain risk identification, Risk response risk owner, controls implemented	Verify that there is a clear and comprehensive procedure for recording, filing, maintaining and reporting on data sources, risk register Determine whether procedures associated with risk management activities are carried out Assess whether all occurrences of risk-related incidents have been reported
6	Risk review	Ensure risk review process is in place and risk review happens periodically for reassessment of identified risks and assessment of new risks	Review risk register for updating after risk review Interview risk owners to confirm they have followed the review process
7	Control identification	Controls should be identified based on the risk assessment. The cost benefit analysis for selected controls must be performed	Check controls selected and implemented are against identified risk Review the cost-benefit analysis (qualitative or quantitative) for implemented controls against total impact/exposure of risk

2. Audit of Security Management

Sl. No.	Audit Area	Test Procedures
1	Security Management framework	Interview senior management on their commitment for information security Check minutes of board meeting, Security reports submitted, reporting frequency of security reports to management Check action and follow up by senior management on security initiatives Verify adequacy of security budget
2	Information security policies	Check whether Information Security Policies have been created, approved by management, and communicated to concerned users. Whether the policy states management commitment and sets out the organisational approach to managing information security. Ensure that security policies have link with risk assessment and suitable policies for organisation's need are appropriately developed.
3	Review of Informational Security Policies	Check whether the Information Security Policies are reviewed at planned intervals, or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness. Check whether the results of the management review are taken into account. Check whether management approval is obtained for the revised policy.
4	Confidentiality And Non-Disclosure Agreements	Check whether the organisation's need for Confidentiality or Non-Disclosure Agreement (NDA) for protection of information is clearly defined and regularly reviewed.
5	Independent review of information security	Check whether the organisation's approach to managing information security, and its implementation, is reviewed independently and periodically or when substantial changes to security policies occur.
6	Identification of risks related to 3rd parties	Check whether risks to the organisation's information and information systems, from 3rd party access, are identified and appropriate control measures implemented before granting access.

Sl. No.	Audit Area	Test Procedures
7	Exception process	Check if the exception process is defined and implemented Verify if exception is against compensating controls and is for limited period of time and management has a plan to close the exceptions Ensure exceptions are reviewed periodically Interview approver for exceptions that they are aware of associated risks.
8	Procedures, standards	Check the internal standards for system configuration, documentation standard, segmentation and security baseline are defined and implemented Review the documented operating procedures for security controls and ensure these are reviewed and updated.

3. Audit of information and asset classification

Sl. No.	Audit Area	Test Procedures
1	Information security policies	Check whether Information Security Policies address the Information and asset classification standards Verify the data/asset classification schema defined by organisation and it is based on the risk assessment Ensure that policy established accountability for asset owners and custodians Interview asset owners and custodians to confirm that they understand their accountabilities. Ensure that policy specifies protection levels for each class of asset.
2	Asset classification process	Review the asset classification process Review the asset inventory including information assets Select sample to review the appropriateness of classification Interview users involved in classification
3	Review of classification	Ensure that asset owners have classified the assets and suitably labelled Check the controls implemented to protect the assets

4. Audit checklist for physical and environmental security

To ensure IS assets are maintained in a secured manner within a controlled environment.

No.	Checkpoints
Secured Physical Access	
1.	Whether Physical Access Control Policy is documented and approved?
2.	Whether the policy on the following is appropriate and covers: Lay out of facilities Physical Security of the assets Access to the assets Maintenance of the assets Signage on the facilities Labels for assets Visitors' authorisation and recording Entrance and exit procedures Legal & regulatory requirements
3.	Whether critical IS facilities (like data centre) are located appropriately? (Verify the location for the following as:- Protection against natural disasters like earthquakes, flooding, extreme weather etc. Not in congested places Not being on ground or top floor Not being below ground level to avoid water leakage etc. Not having a showcase window Not having a direct access from the outside or through a public hallway Place which is not obvious externally).
4.	Whether the access to IS facilities is controlled through a secured mechanism? (Verify the access control mechanism – e.g. access card, lock and key or manned reception).
5.	Whether the access to the IS facilities is limited to approved persons only? (Approved persons may include employees, vendors and customers).
6.	Whether the physical access control procedures are adequate and appropriate for approved persons? (Access should be provided on need to do and need to know basis).
7.	Whether the visitor to critical IS facilities are escorted by employees? (Records for visitors' access should be maintained).
8.	Whether a periodical review of access rights is carried out?
9.	Whether the physical security is continually addressed?
10.	Whether all access routes are identified and controls are in place?
11.	Whether the security awareness is created not only in IS function but also across the organisation?
12.	Whether the physical security is ensured at suppliers' facilities also in cases where organisation's' assets (either physical or data) are processed at supplier's facilities?
13.	Whether the usage of any equipment outside the business premises for information processing is authorized by the management?
14.	Is the security provided to equipment used outside business premises similar to/same as that offered to equipment used inside the business premises?

No.	Checkpoints
15.	Whether adequate monitoring equipment are present to monitor the movements of the personnel inside the facility?
16.	In case of outsourced software, whether all maintenance work is carried out only in the presence of/with the knowledge of appropriate IS staff?
17.	Whether appropriate access controls like password, swipe card, bio-metric devices etc. are in place and adequate controls exist for storing the data/ information on them? Are there controls to ensure that the issue and re-collection of such access devices are authorized and recorded?
18.	Whether access violations are recorded, escalated to higher authorities and appropriate action taken?
19.	Whether employees are required to keep the critical/sensitive documents in secured places?
20.	Check if facility IS related risks with respect to lighting, building orientation, signage and neighbourhood characteristics are identified?
21.	Do the network, operating system and application monitoring procedures provide ample information to identify associated risks?
22.	Verify that surveillance systems are designed and operating properly?
23.	Ensure that physical access control procedures are comprehensive and being followed by security staff.
24.	Verify if the security controls in place are appropriate to prevent intrusion into sensitive IS facilities–data centre, communication hubs, emergency power services facilities?
25.	Review facility monitoring measures to ensure that alarm conditions are addressed promptly.
Environmental Controls	
1	Whether the Environmental Control policy is documented and approved?
2	Whether IS facilities are situated in a place that is fire resistant? (Verify for wall, floor, false ceiling, furniture and cabling being non-combustible/fire resistant/fire retardant).
3	Whether smoking restrictions in IS facilities are in place?
4	Whether adequate smoke/temperature detectors are installed, connected to the fire alarm system and tested?
5	Whether fire instructions are clearly posted and fire alarm buttons clearly visible?
6	Whether emergency power-off procedures are laid down and evacuation plan with clear responsibilities in place?
7	Whether fire prevention and control measures implemented are adequate and tested periodically?
8	Whether fire drill and training are conducted periodically?
9	Whether air-conditioning, ventilation and humidity control procedures are in place, tested periodically and monitored on an ongoing basis?
10	Whether an adequate alternate power arrangement is available? If so, is it covered under maintenance?

No.	Checkpoints
11	Whether alternative water, fuel, air-conditioning and humidity control resources are available?
12	Check if heating, ventilation, and air-conditioning systems maintain constant temperatures within a data centre and other IS facilities?
13	Evaluate the data centre's use of electronic shielding to verify that radio emissions do not affect computer systems or that system emissions cannot be used to gain unauthorized access to sensitive information.
14	Verify if there are sufficient battery backup systems providing continuous power during momentary black-outs and brown-outs along with generators that protect against prolonged power loss and are in good working.
15	Ensure that a fire alarm is protecting a critical IS facility like data centre from the risk of fire, a water system is configured to detect water in high-risk areas of the data centre and a humidity alarm is configured to notify data centre personnel of either high or low-humidity conditions.
16	Check logs and reports on the alarm monitoring console(s) and alarm systems which are to be monitored continually by data center/IS facility personnel.
17	Verify that fire extinguishers are placed every 50th within data centre isles and are maintained properly with fire suppression systems are protecting the data centre from fire.
18	Whether there are emergency plans that address various disaster scenarios for example backup data promptly from off-site storage facilities?
19	Ensure if there exists a comprehensive disaster recovery plan that key employees are aware of their roles in the event of a disaster and are updated and tested regularly.
20	Ensure that detail part inventories and vendor agreements are accurate and current and maintained as critical assets.

Some key tips

1. Physical security is usually the first line of defence against natural/environmental risks and unpredictable human behaviour.
2. Automated environmental controls help minimise the resulting damage and speeds up the recovery process. Manual controls, on the other hand, can be time consuming and error prone.
3. If any physical security controls conflicts with life safety then this issue needs to be addressed; human life is always more important than protecting a facility or the information assets it contains.
4. HVAC should maintain appropriate temperature and humidity levels; provide closed-loop recirculating air conditioning, and positive pressurisation and ventilation.
5. High humidity can cause corrosion, and low humidity can cause static electricity.
6. Emergency procedure documentation (including Disaster Recovery Plan) should be readily available and periodically reviewed and updated.
7. Interior partitions may not go all the way up to the ceiling; as, an intruder can remove a ceiling tile and climb over the partition into a critical portion of the facility.

8. CCTV enables one person to monitor a large area, but should be coupled with alerting functions to ensure proper response.
9. Company property should be marked clearly, and security guards should be trained how to identify when these items leave the facility in an improper manner.
10. Piggybacking, when unauthorised access is achieved to a facility via another individual's legitimate access, is a common concern with physical security.
11. There can be two power source-Primary and Alternate. The primary power source is what is used in day-to-day operations, and the alternate power source is a backup in case the primary source fails.
12. Brownouts may also be the result of power companies facing excessive power demand.
13. Power noise is a disturbance of power and can be caused by electromagnetic interference (EMI) or radio frequency interference (RFI).
14. Power regulators helps condition the line to keep voltage steady and clean.
15. Shielded lines protect from electrical and magnetic induction, which causes interference to the power voltage.
16. Fire detectors should be located below raised floors, on and above suspended ceilings, and in air ducts to provide maximum fire detection.
17. The HVAC should be turned off before activation of a fire suppressant to ensure that it stays in the affected area and smoke is not spread to other areas.
18. Dry pipe systems reduce the accidental discharge of water because the water does not enter the pipes until an automatic fire sensor indicates that there is an actual fire. In locations with freezing temperatures where broken pipes cause problems, dry pipes are preferred.
19. Gases, like halon, FM-200, and other halon substitutes, interfere with the chemical reaction of a fire. Halon is no longer available because it depletes the ozone. FM-200 or other similar substances are used instead of halon.

5. Audit Checklist on Logical Access Controls

The following is an illustrative questionnaire that could be used to review Logical Access Controls within operating systems and databases

No.	Checkpoints
	User Access Management Policy and Procedure
1.	Whether the user access management policy and procedure are documented?
2.	Whether the user access management policy and procedure are approved by the management?
3.	Whether the user access management policy and procedure document includes: Scope and objective. Procedure for user ID creation, approval, review, suspension, and deletion. Granting access to third parties. Password management.

No.	Checkpoints
	User access rights assignment & modifications. Emergency access Granting. Monitoring access violations. - Review and update of document.
	User Access Management
1.	Whether User ID & access rights are granted with an approval from appropriate level of IS and functional head? (Verify the user ID creation, granting of access right and approval process)
2.	Whether the organisation follows the principle of segregation of duties adequately in granting access rights? (Verify Access rights should be given on need to know and need to do basis – without unchecked concentration of power.)
3.	Whether User IDS are in a unique format? (Verify the naming conventions for the user IDs)
4.	Whether invalid log in attempts are monitored and User IDs are suspended on specific attempt? (Verify the parameters set for unsuccessful log in attempt)
5.	Whether the organisation follows complex composition for password parameters? (Complex composition of password parameter should be used as to make it difficult for guess and prevent unauthorised users from access e.g. special character and numbers should be part of password, Restrict use of organisation’s name, 123, xyz or other generic terms as password).
6.	Whether granting access to the third parties is according to the User Access Management policy and procedure? (The organisation should specify and implement a process for granting access to third parties like contractors, suppliers, auditors, consultants etc.)
7.	Whether users are forced to change password on first log-on and at periodic intervals? (Verify password parameters for first log on and password aging).
8.	Whether the organisation implemented clear screen and clear desk policies? (Terminals should be automatically logged off if remaining idle for specific time.)
9.	Whether the organisation restricted concurrent log-on? (One user ID should not be allowed to be logged-in for two different terminals at the same time)
10.	Whether users’ IDs are shared? (Verify whether users’ IDs are shared among the employees/ users or not?)
11.	Whether multiple user IDs are allocated to a single individual?
12.	Are user access policy and procedure documents communicated/available to the respective users?
13.	Whether User IDs and Password are communicated to the user in a secured manner? (Verify the procedure for communicating user ID and password for the first time and after suspension).
14.	Whether the organisation reviews user IDs and access rights at periodic intervals?

No.	Checkpoints
15.	Whether the organisation monitors logs for the user access?
16.	Whether policy and procedure documents reviewed and updated at regular intervals?
17.	Whether the access to scheduled job is restricted to the authorised?
18.	Whether an emergency user creation is according to the policy and procedure for User Access Management? (Verify the emergency access granting procedure, including approvals and monitoring).
19.	Whether periodic review process ensures user accounts align with business needs and removal on termination/transfer? (Review and evaluate procedures for creating user accounts and ensure that accounts are created only when there's a legitimate business need and that accounts are removed or disabled in a timely fashion in the event of termination or job change.)
20.	Whether passwords are shadowed and use strong hash functions? (Ensure the strength of passwords and access permission to password files. Review and evaluate the strength of system passwords and the use of password controls such as aging.)
21.	Review the process for setting initial passwords for new users and communicating those passwords and evaluate the tracking of each account to a specific employee.
22.	Whether the use of groups and access levels set for a specific group determines the restrictiveness of their use? (Evaluate the use of passwords, access rights at the group level)
23.	Ensure that the facility to logon as super/root user is restricted to system console for security reasons.
24.	Check whether the parameters to control the maximum number of invalid logon attempts has been specified properly in the system according to the security policy.
25.	Check whether password history maintenance has been enabled in the system to disallow same passwords from being used again and again on rotation basis.
26.	Verify the parameters in the system to control automatic log-on from a remote system, concurrent connections a user can have, users logged on to the system at odd times (midnight, holidays, etc.) and ensure whether they have been properly set according to security policy.
	Maintenance of sensitive user accounts
1.	Ascertain as to who is the custodian of sensitive passwords such as super/root user and verify if that person is maintaining secrecy of the password, whether the password has been preserved in a sealed envelope with movement records for usage in case of emergency.
2.	From the log file, identify the instances of use of sensitive passwords such as super user and verify if records have been maintained with reason for the same. Ensure that such instances have been approved/ authorised by the management.
3.	From the log file, identify the instances of unsuccessful logon attempts to 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

6. Audit Checklist for Network Administration and Security Auditing

The following is a general checklist for the audit of Network Administration and Security.

No.	Checkpoints
Process	
1.	Is there an Information Security guidelines document, which defines the minimum configuration for any device/link on the organisation's network, including levels of encryption?
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 risk levels are acceptable?
3.	For all items supported by external vendors, does the vendor or the manufacturer verify that all cryptographic functions in use by the product/service, such as encryption, message authentication or digital signatures, use approved cryptographic algorithms and key lengths.
4.	Wherever applicable, whether background and reference checks for both internal and outsourced vendor staff who perform security-related functions for the product/service under review are carried out.
5.	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.
Authentication	
1.	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 then organisation's IT Department? (These include Passwords, Personal Identification Numbers (PINs), (static and dynamic), public keys and biometrics.)
2.	Does the organisation verify that the initial authentication has used a mechanism that is acceptable for the application? Has the approach been approved by IT Department and required compensating controls have been implemented?
3.	Does the organisation have a comprehensive password construction, implementation and management policy?
4.	Do the Products/Services utilising biometrics authentication only use biometrics for local authentication?
Public Key Infrastructure (PKI)	
1.	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?

No.	Checkpoints
2.	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. Are these protections mechanisms adequate?
3.	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. Is such a processes in place?
Access Control	
1.	Is the access to highly privileged IDs (e.g., system administration access) strictly controlled, audited and limited in its use?
2.	Does the product/service support the need to perform a periodic entitlement review? A periodic entitlement review process should validate access privileges.
3.	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?
4.	Is there a process in place to ensure that access rights reflect 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 systems or applications.
5.	For any products/services, which has been outsourced, is there a process in place to ensure that all platforms, services and applications are configured to meet organisation's Information Security Standards?
6.	Does the product/service display the (a) date and time of last successful login and (b) the number of unsuccessful login attempts since the last successful login?
7.	Does the product/service support a periodic process to ensure that all user IDs for employees, consultants, agents, auditors, or vendors are disabled after X days and deleted after Y days from the day they were not used unless explicitly approved by the concerned business manager.
Cryptography	
1.	Is there a cryptography/encryption policy for various types of classified information that travels/gets stored within and outside the organisation's network(s)?
Network Information Security	
1.	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 in place to ensure that the banner is read. The Legal Affairs Banner usually carries the following kind of text: "You are authorised to use this system for approved business purposes only. Use for any other purposes 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. Authorised and unauthorised activities may be monitored."

No.	Checkpoints
	NOTE: This is required for all mainframe, mid-range, workstation, personal computer, and network systems.
2.	Has dial-in connectivity been prohibited on network-connected machine (server and workstation) except where documented and explicitly approved in writing by Business Management and the IT Department. When explicitly approved, the modem must, as a minimum control, prohibit answer or pick up until after the 5th ring.
3.	Have the remote control products used in a dial-in environment been approved by the IT Department explicitly?
4.	Is it ensured that only software (applications /operating systems, etc.) supported by the vendors are used? (Unsupported software could be vulnerable to attacks since the vendors would not come up with the relevant patches.)
Information Security Administration	
1.	Is there an approved document clearly outlining the Security Administrator's (SA) responsibility?
2.	Are all the administrative actions (e.g., adding/deleting users, changes to entitlements/ passwords) backed up by an independent review?
3.	Does the Security Administrator function review all security audit logs, incident reports, and on-line reports at least once per business day?
4.	In case of Wide Area Networks (WAN), are the router tables maintained securely in routers?
5.	Are router login IDs and passwords treated as sensitive information and managed by authorised administrators? Are all changes to router table entries logged and reviewed independently?
6.	Are access violations taken note of, escalated to higher authority and acted upon in a timely manner?
7.	Is there a process to report all unusual or suspicious activity? (Reporting to IT Department, investigating immediately, and bringing the case to closure without delay)?
8.	Does the Security Administrator function assess compliance with their security procedures quarterly and reports their results to the IT Department?
9.	Have all the all security related administrative procedures under the control of the Security Administrator been documented and approved by management (annual exercise)? At minimum procedures should include: Information Ownership Data Classification User registration/maintenance Audit Trail review Violation logging and reporting Sensitive activity reporting Semi-annual entitlement reviews Password resets Escalation reporting

No.	Checkpoints
Microcomputer/PC Security	
1.	Do the LAN servers, mail servers, and microcomputers have IT department approved anti-virus products installed?
2.	Are all product/service specific microcomputers/PCs secured against removal and theft commensurate with the value of the computer and information it holds along with a process to report any thefts to the IT Department?
3.	Are microcomputers / PCs having sensitive information protected with power-on password to prevent unauthorised access?
4.	Are sensitive data in such microcomputers / PCs backed up and preserved properly to ensure recovery in case of failure?
Audit Trails	
1.	Does the audit trail associate with the product/service support the ability to log and review all actions performed by systems operators, systems managers, system engineers, system administrators, highly privileged accounts and emergency IDs?
2.	Does the financial transactions as well as additions, changes and deletions to customer's and vendor's data, get recorded in the product/service audit trail?
3.	Does the audit trail for product/service record all identification and authentication processes? Also is there a retention period for the audit trails? Is it adequate?
4.	Does the audit trail associate with the product/service log all actions by the Security Administrator?
5.	Is there a process to log and review all actions performed by systems operators, systems managers, system engineers, system administrators, security administrators, and highly privileged IDs?
6.	Is there a process in place to log and review actions performed by emergency IDs associated with the product/service?
Violation Logging Management	
1.	Whether the product/service is capable of logging the minimum criteria specified to log and report specific security incidents and all attempted violations of system integrity
2.	Are the product/service owners aware of their responsibilities with respect to Security incident reporting?
Information Storage and Retrieval	
1.	Has all the media (File/Floppy/Disks/Tapes etc.) under the control of the product/service owner been marked with the classification and securely stored with access restricted to authorised personnel only?
2.	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 the data unusable and unrecoverable?

No.	Checkpoints
3.	Is there a procedure in place that enforces and maintains a clean desk programme, which secures all critical information from unauthorised access?
Penetration Testing	
1.	Is it ensured that products/services that use the Internet for connectivity or communications have undergone a successful penetration test prior to production implementation?
2.	Is there a penetration test process that ensures whether modifications to the product/ service that uses the Internet for connectivity or communication have been reviewed to determine whether a subsequent penetration test is warranted?
3.	Is there an intrusion detection system in place for all the external IP connections?

7. Network Infrastructure Auditing Checklist

The following is a general illustrative checklist for the audit of Network infrastructure.

7.1 Network Server

- Obtain or prepare logical and physical diagrams of the network and attached local and wide area networks, including the systems' vendor and model description, physical location, and applications and data residing and processing on the servers and workstations.
- Using the information obtained in the prior steps, document the server and directory location of the significant application programmes and data within the network; document the flow of transactions between systems and nodes in the network.
- Assess whether the trusted domains are under the same physical and administrative control and are logically located within the same sub-network.
- Determine that router filtering is being used to prevent external network nodes from spoofing the IP address of a trusted domain.
- Determine that the Administrator/Super User and Guest accounts have passwords assigned to them (by attempting to log on without providing a password). Also ascertain that the Administrator account password is well controlled and used/known by only the system administrator and one backup person.
- Review the account properties settings active in each user's individual profile, which may override the global account policy.
- List out the security permissions for all system directories and significant application programs and directories and ensure that they are consistent with security policy
- Review and assess permissions assigned to groups and individual accounts, noting that Full Control (all permissions) and Change (Read, Write, Execute, and Delete) permissions are restricted to authorised users.
- Review the audit log for suspicious events and follow up on these events with the security administrator.

7.2 Router

- Determine the types of accounts that were used to access the routers.
- Determine what users had access to these accounts.
- Were access attempts to the routers logged?
- Determine if all accounts had passwords and determine the strength of the passwords.
- Was simple network management protocol (SNMP) used to configure the network?
- Determine the version of SNMP employed by the Company. (Version one stores passwords in clear-text format. Version two adds encryption of passwords.)
- Determine if open shortest path first (OSPF) was defined on the router. Determined the authentication mechanism that was employed in the Company's implementation of OSPF.
- Determine whether directed broadcast functionality was enabled on the router. This setting, if enabled, could allow a denial-of-service (DoS) attack of the network (Smurf attack).
- Obtain population of routers with modems and obtain the telephone numbers of the routers.
- Determine if users were properly authenticated when remotely accessing the routers.
- Determine how changes to the router environment were made.
- Were there procedures for changing router configurations? If so, were these procedures well-documented and consistent with security policy?
- Determine if changes to the router configuration were documented.
- Was there a separation of duties within the change control of the router environment?

7.3 Firewalls

- Obtain background information about the firewall(s), in place, e.g., segment diagrams, software, hardware, routers, version levels, host names, IP addresses, connections, any specific policies for an overview of the firewall security
- Determine that the firewall components, both logical and physical, agree with the firewall strategy.
- Determine whether the firewall components are the latest possible version and security patches are current.
- Determine that the root cannot telnet to the system.
- Determine the telnet OS banner and other banners such as FTP banner, etc. has been eliminated.
- Ensure that there are no compilers/interpreters on the firewall.
- Ensure that a lockdown rule has been placed at the beginning of the rule base. The lockdown rule protects the firewall, ensuring that whatever other rules are put in later, it will not inadvertently compromise the firewall.
- Obtain and review the connections table for time out limits and number of connections
- Attempt to test the rule base by scanning secured network segments from other network segments
- Identify accessible resources behind the firewall that are to be encrypted and determine the connections are encrypted
- Determine if there is a change control process in place for the rule base
- Determine the use of the firewall's automatic notification/alerting features and archiving the detail intruder information to a database for future analysis.

ISBN: 978-81-8441-335-9

₹ 750/- (For Modules I to VII) with DVD

http://cit.icai.org
www.icai.org

1 1 I S A 0 0 2 9
July/2015/P3000(Revised)