ISA

(Modules 1 to 6)

Background Material

INFORMATION SYSTEMS AUDIT 3.0 COURSE

Module - 5

Protection of Information Assets

Digital Accounting and Assurance Board

The Institute of Chartered Accountants of India

(Set up by an Act of Parliament)

New Delhi

Background Material
on
Information Systems Audit 3.0 Course

Module-5 :
Protection of Information Assets

Digital Accounting and Assurance Board

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

Revised Edition	:	August, 2020
Committee/Department	:	Digital Accounting and Assurance Board
Email :		gdaab@icai.in
Website :		www.icai.org/ https://pqc.icai.org
Price	:	₹ 750/- (For Complete Set)
ISBN	:	978-81-8441-995-5
Published by	:	The Publication Directorate on behalf of The Institute of Chartered Accountants of India ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi - 110002
Printed by	:	Sahitya Bhawan Publications, Hospital Road, Agra – 282 003 August | 2020 | P2724 (Revised)

Foreword

The digital revolution is transforming the traditional ways of doing business, necessitating realignment of profession to leverage the multipliers of digital technology - enhanced efficiency, scale and speed, effectiveness, agility and giving access to newer markets. In view of the rapid technological changes, it is imperative for Information System Auditors to adapt, be innovative in aiding organizations to improve its control environment and strengthen governance of IT risks. Adoption of emerging technologies will help them to assimilate vast amount of data and provide value added analysis in the form of data analysis and business intelligence. Chartered Accountants possess unique blend of systems and process understanding and expertise in controls and governance, thereby best suited to be the perfect Information Systems Auditor.

The Institute of Chartered Accountants of India (ICAI), through its Digital Accounting and Assurance Board (DAAB), is continuously monitoring technological developments and taking initiatives to disseminate updated knowledge amongst our members and other stakeholders. In this direction, it is heartening to note that the DAAB is bringing out next version of "Educational Material" for Post Qualification Course on Information Systems Audit. This updated and revised Material combines technology, information assurance and information management expertise that enable Chartered Accountants to be an advisor and handling assurance assignments.

In this updated course curriculum various aspects of emerging technologies like, Blockchain, Robotics Process Automation, etc., have also been introduced to keep members fully abreast. With focus on increased practical aspects, case studies and lab manuals at appropriate places this material is a great learning guide for members aspiring to be Information Systems Auditor.

I compliment CA. Manu Agrawal, Chairman, CA. Dayaniwas Sharma, Vice-Chairman and other members of the Digital Accounting and Assurance Board for generation next material in digital era by taking up this timely initiative.

I am confident that our members would take benefit of these updated modules of post qualification course on Information Systems Audit, so as to render their professional responsibility as Information System Auditor more efficiently and highest standards to achieve global recognition.

CA. Atul Kumar Gupta
President, ICAI

Place: New Delhi

Date: April 12, 2020

Preface

Evolution of digital economy and ever changing dynamic ecosystem presents significant challenges, including new competition, new business and service delivery models, unprecedented transparency, privacy concerns and cyber threats. With a goal to keep members abreast of impact of emerging technologies, Digital Accounting and Assurance Board has come out with the updated Post Qualification Course on Information Systems Audit Modules to equip members with specialised body of knowledge and skill sets so that they become Information Systems Auditors (ISAs) who are technologically adept and are able to utilize and leverage technology to provide reasonable assurance that an organization safeguards it data processing assets, maintains data integrity and achieves system effectiveness and efficiency. This updated syllabus facilitates high level understanding about the role and competence of an IS Auditor to analyse, review, evaluate and provide recommendations on identified control weaknesses in diverse areas of information systems deployment.

Revised Modules of Post Qualification Course on Information Systems Audit has specific objective, i.e., "To provide relevant practical knowledge and develop skills for planning and performing various types of assurance or consulting assignments in the areas of Governance, Risk management, Security, Controls and Compliance of Information Systems." The core of DISA 3.0 lies in inculcating competence to add to service delivery of the members. The updated course would help the members to apply appropriate strategy, approach, methodology and techniques for auditing information system and perform IS Assurance and consulting assignments by using relevant best practices, IS Audit standards, frameworks, guidelines and procedures.

The updated ISA Course 3.0 has a blend of training and includes e-learning, live case studies and lab manuals, project work in addition to class room lectures. This updated background material also includes a DVD which has e-Learning lectures, PPTs, case studies, DEMO CAAT software, useful checklists and sample audit reports. New Module on "Emerging Technology and Audit" has been added which covers Information System Assurance and Data Analytics, Assurance in Block chain Ecosystem, and Embracing Robotic Process Automation in Assurance Services. In addition to this Artificial Intelligence and Internet of Things (IoT) has also been inducted in the new modules.

We would like to take this opportunity to place on record our deep appreciation for the efforts put in by Convener, Dr. Onkar Nath as well as authors and reviewers of the various modules, viz., CA Anand Prakash Jangid, Mr. N.D. Kundu, Mr. Inder Pal Singh, Mr. Avinash Gokhale, CA Pranay Kochar, CA Naresh Gandhi, Dr Manish Kumar Srivastava, Dr. Saurabh Maheshwari, CA Narasimhan Elangovan and CA Atul Kumar Gupta. It would be also appropriate to express our thanks to all the ISA faculties for giving their inputs/ suggestions for the implementation of DISA 3.0.

We would like to express gratitude to CA. Atul Kumar Gupta, President, ICAI, and CA. Nihar Niranjan Jambusaria, Vice President, ICAI, for their thought leadership and encouragement to the initiatives of the Board. We would also like to place on record our gratitude for all the Board members, co-opted members and special invitees for providing their valuable guidance and support in this initiative of the Board. We also wish to express my sincere appreciation for CA. Amit Gupta, Secretary, DAAB, Ms. Nishi Saraf, Section Officer for their untiring efforts in finalization of the updated Modules.

We are sure that these updated Modules on Post Qualification Course on Information Systems Audit would be of immense help to the members and enable them to enhance service delivery not only in compliance, consulting and assurance of IT services, but also provide new professional avenues in the areas of IT Governance, Cyber Security, Information System Control and assurance services.

CA. Manu Agrawal
Chairman
Digital Accounting and Assurance Board

CA. Dayaniwas Sharma
Vice-Chairman
Digital Accounting and Assurance Board

Contents

Learning Objectives

This module focuses on different methods for protecting information assets. This primarily covers following:

- Risk response and definition of controls for protection of information assets
- Essentials of information security management like objectives, processes, policies, procedures, and compliance.
- Information asset protection based on information classification
- Essentials of Physical and environmental security
- Logical access controls
- Network and related security processes.
- Audit guidelines for information protection controls

Chapter 1

Introduction to Protection of Information Assets

1.1 Introduction

It has become imperative for today's organizations to use technology for their business process. Technology has inherent risks and hence it has to be adequately responded with the right level of controls. In order to take benefits of technology, organizations must establish processes for address the associated with technology.

1.2 Risk Response

There are typically four types of risk responses:

1. Avoid: Organization may consider this response by deciding not to use technology for select business operation.
2. Transfer: Where organizations pass on the responsibility of implementing controls 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, organization 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 organizations 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. Organizations may choose to accept remaining risks.

It is possible that organization may select more than one response to manage a risk, for example, organization may choose to implement control (Mitigate) and insure against losses/damage (Transfer). Risk mitigation primarily focuses on designing and implementing controls to prevent incidents due to risk materialization and/or detect when incident happens of likely to happen and define process to recover from incidence.

1.2.1 Information Security Objectives

The overall objective of information security is to protect the information assets and process that supports operations of an organization. This requires maintaining confidentiality, integrity and availability of information system. This is also known as information security triad.

- Confidentiality preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- Availability ensures timely and reliable access to and use of information.

1.3 Threat Modeling Tools

Threat modelling is a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated, and mitigations can be prioritized. The purpose of threat modelling is to provide information professionals with a systematic analysis of what controls or defences need to be included, given the nature of the system, the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker. Attack vector is a path or means by which an attacker can gain unauthorized access to a computer or network to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

1.3.1 OWASP

The Open Web Application Security Project (OWASP) is a non profit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

Globally recognized by developers as the first step towards more secure coding.

Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

1.3.2 DREAD Model

DREAD is part of a system for risk-assessing computer security threats previously used at Microsoft and currently used by OpenStack and other corporations.

It takes into account the following items:

	Categories	Description
D	Damage potential	How many assets can be affected?
R	Reproducibility	How easily the attack can be reproduced?
E	Exploitability	How easily the attack can be launched?
A	Affected users	What is the number of affected users?
D	Discoverability	How easily the vulnerability can be found?

The DREAD name comes from the initials of the five categories listed above. It was initially proposed for threat modeling, but it was discovered that the ratings are not very consistent and are subject to debate. It was out of use at Microsoft by 2008.

When a given threat is assessed using DREAD, each category is given a rating from 1 to 10. The sum of all ratings for a given issue can be used to prioritize among different issues.

1.3.3 STRIDE Model

The STRIDE model was initially created as part of the process of threat modelling. STRIDE is a model of threats, used to help reason and find threats to a system. It is used in conjunction with a model of the target system that can be constructed in parallel. This includes a full breakdown of processes, data stores, data flows and trust boundaries.

Each following threat is a violation of a desirable property for a system:

	Threat	Desired Property
S	Spoofing	Authenticity
T	Tampering	Integrity
R	Repudiation	Non-repudiation
I	Information disclosure	Confidentiality
D	Denial of service	Availability
E	Elevation of privilege	Authorization

1.4 Cyber/ Computer Attacks

Following are some of the crime and attacks in information system environment:

- Backdoor: A backdoor is a malicious program that listens for commands on a certain TCP or UDP port. Most backdoors allow an attacker to perform a certain set of actions on a host, such as acquiring passwords or executing arbitrary commands. Types of backdoors include zombies (better known as bots), who are installed on a host to cause it to attack other hosts, and remote administration tools, which are installed on a host to enable a remote attacker to gain access to the host's functions and data as needed. Use of licensed software, patch updates, disabling default users & debugging function and using anti-malware software are the controls against backdoor.
- Blue Jacking: It is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard, which typically contains a message in the name to another Bluetooth-enabled device. Turning off Bluetooth, selecting hidden mode, and ignoring and/or deleting messages, can prevent blue jacking.
- Buffer Overflow: A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. This is a special case of the violation of memory safety. Developing security measures in the code and run-time protection features of most of the operating systems are controls for buffer overflow.
- Cyber Stalking: It is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, or gathering information that may be used to threaten, embarrass or harass. Maintaining cyber hygiene and avoid disclosing sensitive information are preventive controls.
- Cyber Terrorism: is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. Passive defense for this attack is essentially target hardening.
- Cyber Warfare: It is the use of technology to attack a nation, causing comparable harm to actual warfare. Limiting employee access to classified information and installing software updates may help to prevent this attack.
- Data Diddling: Data 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. File encryption or some type of integrity checks such as checksum or message digest may prevent such attacks.
- Denial of Service: A Denial-of-Service attack (DoS) is an attempt to make a machine or network unavailable to its intended users. This causes legitimate users not able to

get on the network and may even cause the network to crash. Web application firewall software may help to prevent DOS attack.

- DNS Spoofing: It is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer). Keeping resolver private and protected is one of the controls against DNS spoofing.
- Email Spoofing: It is the creation of email messages with a forged sender address. The core email protocols do not have any mechanism for authentication, making it common for spam and phishing emails to use such spoofing to mislead or even prank the recipient about the origin of the message. Configuring reverse proxy may detect e-mail spoofing in most of the cases.
- Identity Theft: It is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss. The person whose identity has been assumed may suffer adverse consequences, especially if they are held responsible for the perpetrator's actions. Use of strong password, multi factor authentication, monitoring transactions of the account are some of the preventive controls.
- Keystroke Logger: A keystroke logger monitors and records keyboard use. Some require the attacker to retrieve the data from the host, whereas other loggers actively transfer the data to another host through email, file transfer, or other means. Use of key encryption software and installing anti malware may prevent this attack.
- Logic Bomb: These are legitimate programs, 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 program is run, the logic bomb checks external environment to see whether the condition to trigger the bomb has been met. Anti-malware and use of application from trusted source may be preventive controls.
- Piggybacking: Unauthorized access to information by using a terminal that is already logged on with an authorized ID (identification) and left unattended. In this case, idle session timeout (i.e. disabling session after specific time period) may be a preventive control.
- Salami Theft: It is a series of minor attacks those together results in a larger attack. Computers are ideally suited to automating this type of attack. By having proper segregation of duties and proper control over code, organization may prevent this.
- Sensitive Data Exposure: Many web applications and APIs (Application Program

Interface) do not properly protect sensitive data, such as financial, healthcare, and PII (Personally Identifiable Information). Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser. Data leakage prevention tools may prevent sensitive data exposure.

- Injection: Injection flaws, such as SQL, NoSQL, 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. Input validation, security audits and vulnerability, threat and risk (VTR) assessment may help to prevent injection attacks.
- Trojan: A Trojan horse is a self-contained, no replicating program that, while appearing to be benign, actually has a hidden malicious purpose. Trojan horses either replace existing files with malicious versions or add new malicious files to hosts. They often deliver other attacker tools to hosts. Sound policies and procedures should be in place and anti-malware software should be installed.
- Virus: A virus self-replicates by inserting copies of itself into host programs or data files. Viruses are often triggered through user interaction, such as opening a file or running a program. Sound policies and procedure should be in place and anti-malware software should be installed. Viruses can be divided into the following two subcategories:
    - Compiled Viruses: A compiled virus is executed by an operating system. Types of compiled viruses include file infector viruses, which attach themselves to executable programs; boot sector viruses, which infect the master boot records of hard drives or the boot sectors of removable media; and multipartite viruses, which combine the characteristics of file infector and boot sector viruses.
    - Interpreted Viruses: Interpreted viruses are executed by an application. Within this subcategory, macro viruses take advantage of the capabilities of applications' macro programming language to infect application documents and document templates, while scripting viruses infect scripts that are understood by scripting languages processed by services on the OS.
- Worm: A worm is a self-replicating, self-contained program that usually executes itself without user intervention. Sound policies and procedure should be in place and anti-malware software should be installed. Worms are divided into two categories:
    - Network Service Worms: A network service worm takes advantage of vulnerability in a network service to propagate itself and infect other hosts.

    - Mass Mailing Worms: A mass-mailing worm is similar to an email-borne virus but is self- contained, rather than infecting an existing file.
- Web Defacement: It is an attack on a website that changes the visual appearance of a website or a web page. These are typically the work of defacers, who break into a web server and replace the hosted website with one of their own. Security audits and vulnerability, threat and risk (VTR) assessment are controls for this attack.

1.5 Information Systems Controls

Control is defined as a mechanism that provides reasonable assurance that business objective will be achieved and undesired events are prevented, detected or 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 system auditing includes reviewing the implemented system or providing consultation and evaluating the reliability of operational effectiveness of controls.

1.5.1 Need for Control

Use of information system has become imperative for businesses. Information system 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 organization. Safeguarding information assets to maintain confidentiality, integrity and availability to achieve system effectiveness and efficiency is a significant control process.

The factors influencing an organization for control and audit of the information systems are as under:

- Organizational Costs of Data Loss.
- Incorrect Decision Making
- Costs of Computer Abuse
- High Costs of Computer Error
- Maintenance of Privacy
- Controlled evolution of computer Use
- Information Systems auditing
- Asset Safeguarding

- Data Integrity
- System Effectiveness
- System Efficiency

1.5.2 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 serves two main purposes:

- Outline the policies of the organization as laid down by the management.
- 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 exploiting vulnerability. Some categories of exposures are:

- Errors or omissions in data, procedure, processing, judgment and comparison.
- Improper authorizations 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 computerized 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 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 information system implementations or inadequate security functionality in information system.

1.5.3 Internal Controls

The basic purpose of an internal control in an organization is to ensure that the business

objectives are achieved and undesired risk events are prevented or detected and corrected. This is achieved by designing an effective internal control framework, which comprises policies, procedures, practices, and organizational structure that gives reasonable 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 organization.

1.5.4 Types of Internal Controls

There are three types of internal controls viz. preventive, detective, or corrective (reactive):

1.5.4.1 Preventive Controls

These controls are designed to create a desired level of resistance and its goal is to prevent the attack actively. These controls are directly related to the resiliency aspect of the information systems. Input validation, patching, intrusion prevention system (IPS) are some of the example of preventive controls.

1.5.4.2 Detective Controls

These controls are designed to build a historical evidence of the events or activities in the information system environment. These controls are directly related to the reliability aspect of the information systems and in general passive in nature. Recording audit logs, Hash value, intrusion detection system (IDS) are some of the example of detective controls.

1.5.4.3 Corrective Controls

These controls are designed to reduce the impact or correct an error once it has been detected. These controls are directly related to bringing back business operations to normal and reactive in nature. Load balancing, clustering, failover of data and system, contingency planning are some of the examples of corrective controls.

The controls rating by an auditor can be:

- Very High- Controls are implemented over a cause of exposure/error type and are extremely effective.
- High- Controls are implemented over a cause of exposure/error type and are highly effective.
- Moderate- Controls are implemented over a cause of exposure/error type and are moderately effective.
- Low-Controls are implemented over a cause of exposure/error type but have low effectiveness.
- Negligible- Controls are not implemented or do not exist to that cause or exposure or error type.

1.6 Risk and Control Ownership

Each risk should have an owner, and the owner should determine the controls that are necessary to mitigate the risks. Generally, owner is a person or position within the organization that has close interests in the processes affected due to risks. The concept of a direct link between risk and control is important to ensure that all risks have been addressed through appropriate controls and that all controls are justified by the risks that mandate the requirements for those controls.

The owner/s of the risk/s also own any control/s associated with those risks and is accountable for monitoring their effectiveness. In some areas, where there are regulations or laws that apply to risks, the risk owner may have to prepare standard reports on the status of risks, any incidents that may have occurred and the level of risks currently faced by the organization.

1.7 Periodic Review and Monitoring of Risk and Controls

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

- The risk assessment exercise may be conducted after predefined period say at least annually.
- All incidents and lesson learned must be used to review the identified risk
- Change management processes should proactively review the possible risks and ensure that they are part of organization's risk register.
- New initiatives and projects must be considered only after risk assessment.

1.7.1 Controls Assessment

The first step in controls assessment is to review the risk register and ensure that associated risk is responded appropriately. Based on this the auditor shall be able to prioritize the controls to be tested. The next step is to review control procedure documents with an aim of identifying suitable ways of measuring the effectiveness of controls.

1.7.2 Control Self-Assessment

Control self-assessment (CSA) is a technique that allows business managers and employees directly involved in business units, functions or processes to participate in assessing the organization's risk management and control processes. In case organization 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 organization 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 methods can be used for risk assessment and control design.

1.7.3 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 an Auditor, to provide objective assurance to the board on the effectiveness of an organization'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 IS auditor, plan the audit cycle according to the perceived risk, i.e. plan for higher frequency for high-risk business processes areas.

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 activities, 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.

1.8 Summary

Information Security is a paramount risk management concern. Information Risk Management follows information as it is created, distributed, stored, copied, transformed and interacted throughout its lifecycle. It includes understanding which information is critical to key business initiatives, such as growth through acquisitions or expanding partnerships, where it exists across the organization, where the points of vulnerability are, and what events could put the business at risk. Investments are prioritized based on the amount of risk a given activity entails relative to the potential business reward, and in keeping with the organization'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.

1.9 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. Organizations 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 organization?

   A. Management decides to acquire new application software.

   B. A new application required by organization is released.

   C. Vendor decides to stop supporting existing application.

   D. Organization 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.

1.10 Answers and Explanations

1. B is the correct answer. 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 is the correct answer. Of the four main risk response options accept, avoid, mitigate and transfer, Insurance cover is a risk response option of risk transfer

3. B is the correct answer. BY shifting location, the business has avoided the risk associated with Tsunami.

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

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

6. B is the correct answer. 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 is the correct answer. Vendor decides to stop supporting existing software changes the market situation that will affect organization, since it has to take decision on replacing application. Release of new application though changes market; it may not

affect the organization immediately as the organization 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 is the correct answer. 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 is the correct answer. 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 is the correct answer. 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

Administrative Controls of Information Assets

2.1 Information Security Management

Protection of information assets includes the key components that ensure confidentiality, integrity and availability (CIA) of information assets. 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. Organization needs to focus on ensuring that information security procedures are followed to meet the security objectives of the organization derived from the stakeholder's expectations. This requires implementation of processes for information security management. The key elements of information security management include:

- Senior management commitment and support,
- Policies and procedures,
- Organization structure and roles and responsibilities,
- Security awareness and education,
- Monitoring,
- Compliance,
- Incident handling and response.
- Continual improvement

2.2 Senior Management Commitment and Support

Commitment and support of senior management are imperative for successful establishment and continuance of an information security management program. The tone at the top must be conducive for effective information protection and its management. It is unreasonable to expect shop-floor personnel to abide by information security policies, if senior management does not exercise them. Executive management endorsement of essential security requirements provides the basis for ensuring that security expectations are met at all levels of the enterprise. Disciplinary actions for non-compliance must be defined, communicated and enforced from the senior management level. The senior management's support for security initiatives is evident from their actions and decisions. Some of the key indicators are:

- Providing support for defining organization structure that supports implementation of

information security initiatives. Establishing Information Security Organization (ISO) and steering committee and assigning responsibility for information security operations.

- Regularly reviewing information security projects, reports and activities as part of an agenda item on board meetings.
- Approving risk response decisions and information security policies.
- Observing security practices, as per security policies and procedures
- Ensuring adequate budget
- Review of audit reports
- Continual improvement

2.3 Critical Success Factors to Information Security Management

Following are critical to the successful implementation of information security program in the organization:

- Alignment with business objectives: The Management needs to establish security policy in line with business objectives, to ensure that all Information Security elements are strategically aligned.
- Organizational culture: Ensure that the framework followed to implement, maintain, monitor and improve Information Security is consistent with the organizational culture.
- Establish and enforce an information security program: The focus of information security program is protecting information assets of the organization. Management should establish and enforce information security program enterprise-wide.
- Adoption of standard: Adoption of standard or framework may enable organization to have consistent implementation across the enterprise. This also helps in providing assurance that all required aspects of information security have been covered. Many a time regulators issue guideline for adoption and certification of standards/ framework available in public domain.
- Spend resources wisely and transparently: Expenditures on controls to mitigate risks should be prioritized and unnecessary resource utilization may be avoided.

2.4 Information Security Organization

Information security is responsibility of entire organization and accountability of senior management and board of director. Chief Information Security Officer (CISO) is facilitator in implementing security across organization. The CISO plays a critical role in ensuring

protection of an Organization's information and information assets, privacy of information, managing vulnerabilities, responding to incidents, and compliance of policies, training and awareness of policies.

The position must be strategically placed within the Organization 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 Organization's business is critical to a CISO's success.

To ensure that information security is implemented across organization CISO requires creation of the information security organization. This can be best done by defining security responsibilities for every person and position as part of his/her role within organization and documented in their job description. While defining roles and responsibilities following aspects must be considered.

2.4.1 Segregation of Duties

Segregation of duties is the concept of having more than one person required to complete a task. In business, the separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud and error. In essence, SoD implements an appropriate level of checks and balances upon the activities of individuals. A programmer should not be allowed to operate a computer system, or to gain access to production systems or data. Similarly, operators should not act as programmers although, in practice, this rule is becoming undermined by the use of personal computers and small office systems and in tiny/small companies.

2.4.2 The 'Four Eyes' (Two-Person) Principle

This is one of the central principles of authorization in the information systems of financial organizations. The principle of maker and checker means that for each transaction, there must be at least two individuals necessary for its completion. While one individual may create a transaction, the other higher designation should be involved in confirmation/ authorization of the same. Here the segregation of duties plays an important role. In this way, strict control is kept over system software and data, keeping in mind functional division of labour between all classes of employees. In some business systems (e.g. SWIFT), it is necessary to have "six eyes" principle i.e. maker-checker-approver.

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 maker and checker. Vital functions should be well dispersed amongst staff members. Although this can be seen, as mistrust to staff but may provide protection too.

2.4.3 Rotation of Duties

Some employers to rotate their employees' assigned jobs throughout their employment use this technique. Employers practice this technique for a number of reasons. It was designed to promote flexibility of employees and to keep employees interested into staying with the company/ organization, which employs them. There is also research that shows how job rotations help relieve the stress of employees who work in a job that requires manual labour. Rotation of duties may also 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 should take at least two consecutive weeks holiday in every year as industry experience has shown that many frauds need continual masking by the perpetrator and may surface when the individual is away.

2.4.4 'Key Man' Policy

Key employee or key man is a term used specifically for an important employee or executive who is core to the operation of the business and his death, disability or absence could prove to be disastrous for the company or organization. In cases where a single individual is critical to the business, 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 organization, should there be an accident.

2.5 Information Security Policies, Procedures, Standards and Guidelines

Information Security policy will define management's intent on how the security objectives should be achieved. It will also encompass the view on risk and will define security initiatives/controls to meet business objectives. Information security policies, guidelines and procedures affect the entire organization 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 adopted/defined to set the mandatory rules that will be used to implement the policies. A standard is typically a collection of system-specific or procedural-specific requirements that must be met by everyone. Procedures are the detailed activities for implementation of policies.

Every policy should have corresponding procedures. Some policies may have multiple guidelines, which are recommendations as to how the policies can be implemented smoothly. A guideline is typically a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended. Effective security policies make frequent references to standards and guidelines that exist within an

organization. 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 organization and discusses the information assets that need protection and the extent to which protection is required. The Information Security Policy is an overview or generalization of an organization'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 assessment process. Organizations may have polices depending upon culture of organization, nature of business, compliance requirements, geographical and regional environment within which organization is operating.

2.5.1 Components of Information Security Policies

- Statement
- Scope
- Objective
- Ownership
- Roles and Responsibility
- Business requirement of Information security
- Policy Exceptions
- Compliance
- Periodic review

2.5.2 Other Common Security Policies

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

Data Classification and Privacy Policies

It is the policy of the Organization to protect against the unauthorized 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 organization 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 authorized to receive it.
- The organization shall adopt procedures for the administrative, technical and physical safeguarding of all non-public personal information.

- The organization shall ensure that an entity controlled by it, or any other entity that utilizes information provided by the organization 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 organization 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 that restrict the ways in which the information resources (Data, Application Systems, Technology, Facilities and People) may be used. AUP often reduces 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 organization to sign an AUP before they are given access to its information systems. For e.g. it may state that no user of company's Internet facility will use for personal purpose.

Physical Access and Security Policy

Physical security describes security measures that are designed to restrict unauthorized access to facilities, equipment and resources, and to protect personnel and assets 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 business requirements for Information assets protection. It includes assets like servers, desktops, handhelds, software, network devices etc. Besides, it covers all assets used by an organization- owned or leased. E.g., asset management involves asset acquisition, identification, storage, movement, accounting, disposal etc.

Network Security Policy

A network security policy defines the overall rules for organization'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 organization to access the information assets. For example:

- Password length must be more than 8 characters

- Password must meet complexity requirements, such as upper case, lower case, numeric and special characters
- Password must have defined maximum age
- Password must have defined minimum age
- Password must have history control

2.5.3 Controls over Policy

Information security policies need to be maintained, reviewed and updated regularly. This is required due to changes in environment, information technology, threat scenarios, business processes, business strategy, and organizational structures. It is necessary to review the security policies periodically to ensure that they are in line with the senior management's intent. Typically, security policies are reviewed:

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

2.5.4 Exceptions to the Policy

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 level. Such exceptions should be for a predefined period, must be removed when stipulated period and 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 should be modified to comply with password policy.

2.6 Information Classification

Data is a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. It is held by the company on its own behalf and/or is entrusted to it by others. It is also information (original or derived) organized for analysis or used to make decisions.

Information classification can provide organizations with a systematic approach to protect information consistently across the organization 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 organization is expected to protect information, during its lifecycle in a consistent manner. The state in which information exists can also influence how a piece of information should be protected.

2.6.1 Benefits from Information Classification

- 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 unauthorized disclosure, theft and information leakage)
- Information classification can be used to demonstrate that the organization is meeting particular compliance requirements (e.g. Personal Data Protection Bill) and regulation (e.g. RBI)
- Information classification helps to ensure that security controls are only applied to information that requires such protection. This may reduce the cost of protecting information.
- 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)

2.6.2 Information Classification Policy

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

- Objective of classification of information assets
- Structure of classification schema (categories of classes)
- Information owners and custodians
- Protection levels for each class of information defined by schema
- Classification method using impact on business if information is breached or not available and possibility (Likelihood) of breach.
- Policy also determines the responsibility and 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 organization.
- Where practicable, the information classification shall be embedded in the information itself.

2.6.3 Classification Schema

Most organization may follow following classes: Top secret, confidential, sensitive, internal and public. Following table describes the general description of classification schema, however organization may adopt different schema depending upon requirement, nature of business, compliance requirements etc.

Information Category	Description	Example
Unclassified/ Public	When the unauthorized disclosure, alteration or destruction of that data could cause low or no risk	Information widely available in the public domain, including publicly available Company web site areas
Sensitive	When the unauthorized disclosure, alteration or destruction of that data could cause a moderate level of risk	All Company-developed software code, whether used internally or sold to clients
Client Confidential Data	When the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk	Product information generated for the client by company Client's data such as name, age, sex etc., Feedback given by the client
Company Confidential Data	When the unauthorized disclosure, alteration or destruction of that data could cause a highest level of risk	Confidential customer business data and confidential contracts

2.7 The Concept of Responsibility in Information Security

Responsibilities are defined duties of individual within an organization; once a responsibility is assigned, it is usual for an individual to be held responsible for satisfactory performance. The main types of role within an information security structure are given below:

2.7.1 Ownership

Organization has acquired (instead of "has acquired" "acquires") a number of assets required for business operations. The organization 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 not only have right to use the assets but also are responsible for the safekeeping of assets.

Every asset of the organization including the information assets should have a clearly defined

'owner'. The owner should then have a defined set of responsibilities. Authorization is the essential statement where an owner gives their assent to an activity happening.

2.7.2 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 scenario, the owner may delegate responsibility to a custodian. The owner should clearly state the requirements; the responsibilities and associated levels of authority of the custodian on the assets but finally management responsibility will always reside with the owner. Example of custodian is a database administrator.

2.7.3 Controlling

In all information, security areas there are key tasks, which can be called control points. It is at these control points that the actual information security mechanism has its application. For example, a system administrator acts as a control on who has access to information 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.

2.7.4 Human Resources Security

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

The management of human resources security and privacy risks is necessary during all phases of employees' association with the organization. Training and education are intended to individuals with focus to prevent data disclosure, recognize information security problems and incidents, and respond according to the needs of their job role(s). Following are the some of the recommended safeguards:

- Job descriptions and screening,
- User awareness and training,
- A disciplinary process, and
- An exit process must exist to equip employees to operate securely and use information appropriately, and ensure the revocation of access privileges when a user's relationship with the organization ends.

The objectives of human resources security is to ensure that all employees and third parties (having access to organizations' information assets) are qualified 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:

- Pre-employment: It includes defining roles and responsibilities of the job, defining appropriate access to sensitive information for the job, and determining candidate's screening levels - all in accordance with the company's information security policy.
- During employment: Employees and third parties those who have access to sensitive information in the organization should receive periodic reminders of their responsibilities and receive ongoing, updated security awareness training to ensure their understanding of current threats and corresponding information security practices to mitigate corresponding risks.
- Termination or change of employment: To prevent unauthorized access to sensitive information, access must be revoked immediately upon termination/separation of an employee and third parties from the organization. This also includes the return of the assets of the organization.

2.8 Training and Education

Various computer crime studies show that the threat from insider's ranges from 60% to 90%. This does not mean that more than 60% of the employees in an organization are trying to hack into the system. It does also 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 or downloading shareware from the Internet. Thus, employees need to be made aware about the information security policies of the company and how to practice good computer security skills.

An integrated security training, awareness, and education program 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 program 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. Some of the important considerations for security awareness training program are:

- Mandatory security awareness: Ensure that security awareness training is mandatory for all staff (including senior management).
- Training for third parties: Ensure that all third parties who are having access to an organization's information assets should also receive information security awareness training.

- Training is required before access is granted: Security awareness training commences with a formal induction process designed to introduce the organization's information security policies and expectations before access granted to information or services. (I think it should be “first time access” granted, otherwise giving training every time, the access is taken is impossible)
- Acknowledge policy: Ensure that all target audience including the third party have acknowledged that they have read and understood the organization's information security / acceptable use policy.
- Training at least annually: Ensure that all target audience including the third party (having access to company information and information systems) are given security awareness training at least once in a year.
- Cyber security training: Use of Information Technology by banks and their constituents has grown rapidly and is now an integral part of the operational strategies of banks, subsequently; cyber security risk has become part of the business risk. Government and regulators are also directing enterprises to implement controls for cyber security risk and generate awareness at all levels. In the present scenario, in banks, it has become board level agenda. There is need for greater awareness of cyber security risk and issues by the senior management of banks, so as to strengthen cyber resilience. With a view to enhance the management's awareness in banks, of the IT and cyber security issues in a systematic and structured manner, the RBI has designed awareness/certification program customized for senior management. The expectation is that, such a programme will enable senior management to contribute more effectively in the matters relating to implementation, review and monitoring of the cyber security strategy of their bank, by imparting a better appreciation of the ever-evolving cyber risk-threat universe.

2.9 Implementation of Information Security Policies

Appropriate implementation of information security policy helps in minimizing internal security breaches that are accidental and unintentional. Educating employees about the importance of complying information security policies is most important process. In addition, following may help in smooth and successful implementation of information security policies.

2.9.1 Increasing Awareness

The success of information security policy depends upon employee’s understanding and compliance in routine operations. Information security department should understand the level of employee awareness in order to determine the effectiveness of information security policy. In this context, a survey may help to determine the level of employees’ awareness. Some of the aspect regarding which questions may be included in the survey:

- Do employees know that there are security policies?
- Do they know the distribution point?
- Are the policies easily accessible?
- Have all the employees read the policies?
- Do the employees understand the policies?

2.9.2 Communicating Effectively

While explaining security policies to new hires or sharing updates with employees, clear communication through established channels is critical. Ensuring that employees understand the reason to comply with information 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 the annual training.
- Supplement primary communications vehicles with website and newsletter articles.

2.9.3 Simplify Enforcement

The compliance of information security policies should be enforced through the senior management communications. Following dimensions may help in compliance of information security policies in day-to-day operations.

- Creating a manageable number of policies: Keeping the number of policies manageable so users can more easily find the policy that they need in their routine activity.
- Making policies understandable for target audiences: Using language that is suited for target users with examples that how a user shall adhere to the information security policy.
- Making it easy to comply: Including employee's feedback during policy review to get better sense and ease of compliance.
- Integrating security with business processes: Integrating information security policy compliance into business processes, so employees will not need to bypass security procedures while doing business operations.
- Aligning policies with job requirements: Information security policy should be in line with job requirements.

2.9.4 Integrating Security with the Corporate Culture

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

- Making employees a partner in the security challenge: Establish good relationships and use the awareness program to encourage business leaders to drive security within their organizations. 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.
- 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 related training or communication.
- Tying security policies to company's code of business conduct: Educate employees to understand that their compliance with information security initiatives is integral to overall appropriate behaviour and critical to success of business.

2.10 Issues and Challenges of Information Security Management

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

- Organization's strategic drivers: The strategic drivers and needs of the organization may conflict with the actions required to ensure that assets and processes remain productive. Finding the right balance between protecting the organization's core assets and processes and enabling them to do their job becomes a challenge for security management—and a significant barrier to effectiveness.
- Regulatory requirements: Another consideration for information security management is the organization's regulatory environment. Just as the organization must expose itself to its environment to operate, so must it be willing to accept the limitations imposed by regulators. This brings another level of challenges that affects the organization's ability to be effective at security management.
- Information security as an afterthought: The problem of information security is to consider it as an afterthought. Once an information system has been implemented, it is a norm to follow a checklist to understand whether any of the security 'holes' remained unplugged. While the information security community has recognized 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. Checklists are important as a starting point or as a tool to ensure that you are not missing out anything but should not be totally relied upon.

- 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.

2.11 Summary

Information security management has become more important over the years due to increased use of information system for conducting business. Information security management is a business issue and it needs to be properly integrated into the organization's overall business goals and objectives because security issues may negatively affect the resources, which is(remove "which is") having dependency on the organization. The objectives of information security are to provide confidentiality, integrity and availability to data and resources. The need for complex networks is due to complexity of business operations and delivering products and services to the customers. These networks have evolved from centralized environments to distributed environments.

2.12 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. Information security policies are set of various policies addressing different information systems areas based on the IT infrastructure of organization. Which of the following policy is most common in all organizations?
   - A. Acceptable use policy

B. BYOD (Bring Your Own Device) policy

C. Data encryption policy

D. Biometric security policy

4. 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

5. 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

6. 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

7. 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

8. 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

9. 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?
10. Which of the following best helps in classifying the information within organizations?
   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

2.13 Answers and Explanations

1. A is the correct answer. The primary objective of information security management is to provide adequate level of protection to information security assets.
2. B is the correct answer. Policies are vehicle to communicate management's intent to all stakeholders. Information security practices are aligned with business objectives and not with the strategy. Information security policies are defined as outcome of risk assessment. Compliance with standard is not primary function of policies.
3. C is the correct answer. Acceptable use policy that address the use of information assets by users is most common in all organizations that depends upon IT. Policies in other option depend upon organization's use of BYOD or Encryption or Biometric.
4. C is the correct answer. Integrity primarily refers to reliability that is achieved by implementing controls to ensure accuracy and completeness of data.
5. C is the correct answer. Changes in environment introduce new risks. In order to address them it is necessary to review the information security policy based on assessment of new risks. Other options are secondary reasons.
6. D is the correct answer. Without senior management's support, information security cannot have a success. Senior management is involved many activities in effective information security initiative. Reviewing progress of information security in monthly meeting is one of them. Other options may or may not indicate unless there is more evidence to conclude.
7. B is the correct answer. Policy exceptions are temporary and must be reviewed and closed as per defined plan. Increased number of exceptions indicates that the policy

provisions may not be appropriate and hence need to be reviewed. Other options are not concerning.

8. C is the correct answer. Primary purpose of information classification is to provide appropriate level of protection to information assets. Options A, B and D are the secondary with respect to information classification.

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

10. B is the correct answer. 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 organization's objectives. C and D are performed after classification of information.

Chapter 3
Physical and Environmental Controls

3.1 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 organization. Today, there is a computer on almost every desk, and access to devices and resources is spread throughout the environment, besides, organizations have several remote and mobile users.

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 non-availability of technology. This means the environment must be able to provide and sustain climatic conditions like appropriate level of temperature and humidity, dust free environment.

3.2 Objectives of Physical Access Controls

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 information resources from physical access exposures. 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.

3.3 Physical Security Threats and Exposures

3.3.1 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 unauthorized personnel
- Authorized personnel having pre-determined rights of access, misusing their rights in a manner prejudicial to the interests of the organization
- Authorized personnel gaining access to information systems resources for which they are not authorized. (i.e. gaining access to resources beyond their rights of "need to know; need to do")
- Interested or Informed outsiders such as competitors, thieves, organized 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

3.3.2 Physical Access Exposures to Assets

- Unintentional or Accidental: Authorized personnel or unauthorized personnel unintentionally gaining physical access to IS resources.
- Deliberate: Unauthorized personnel may deliberately gain access or authorized personnel may deliberately gain access to information resources, for which they are not permitted or do not possess rights of access.
- Losses: Improper physical access to IS resources may result in losses to organization, which can result in compromising confidentiality, Integrity and availability of information system resources.

3.4 Physical Security Control Techniques

Define physical security controls and protection levels at each layer (viz. Deterrence, Access Control, Detection and Identification):

3.4.1 Choosing and Designing a Secure Site

Organizations may have following consideration during initial planning for information processing facility (IPF) or data centre site:

- 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.
- 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.
- 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.

3.4.2 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 when access attempts occurred and who attempted them. The audit trails or access logs must record the following:
    - The date and time of the access attempt
    - Whether the attempt was successful or not
    - Where the access was granted (which door, for example)
    - Who attempted the access?
    - Who modified the access privileges at the supervisor level?
- Reporting and incident handling procedure: Once an unauthorized event is detected, appropriate procedures should be in place to enable reporting of such incidents and effectively handling 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.

3.4.3 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.

3.4.4. Human Resource Controls

These includes identification of employees and visitors, providing identity cards, assigning responsibilities, provided training in physical security, monitoring behaviour, escorting terminated or resigned / retired employees. 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.

3.4.5 Perimeter Security

- 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.
- Dogs: Dogs are used in perimeter security, they are reliable, and have a keen sense of smell and hearing. However, they cannot make judgment calls the way humans can.
- Compound Walls and Perimeter Fencing: A common method of securing against unauthorized boundary access to the facility. It helps in deterring casual intruders but is ineffective against a determined intruder.
- 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.
- Dead Man Doors: Dead man doors use a pair of doors. For the second door to operate, the first entry door must close and lock so that only one person is permitted in the holding area. This effectively reduces the risk of piggybacking.
- Bolting Door Locks: This is the most commonly used means to secure against unauthorized access to rooms, cabins, and closets. It requires traditional metal key to gain entry. Unauthorized individuals could still gain access to the processing center along with an authorized individual. This is cheap yet a reasonably effective technique, however control over physical custody and inventory of keys is required.

- Combination or Cipher Locks: Combination door locks, also known as cipher locks, use a numeric keypad or dial to gain entry. They do not prevent or reduce the risk of piggybacking since unauthorized individuals may still gain access to the restricted area.
- Electronic Door Locks: Such locks may use electronic card readers, smart card readers or optical scanners to gain entry. They do not prevent or reduce the risk of piggybacking, since unauthorized individuals may still gain access to the restricted area.
- Biometric Door Locks: These are some of the most secure locks since they enable access based on physiological features such as voice, fingerprint, hand geometry, retina or iris. However, they do not prevent or reduce the risk of piggybacking.
- Perimeter Intrusion Detectors - The two most common types of physical perimeter detectors are based on either photoelectric sensors or dry contact switches.
    - 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.
    - Dry Contact Switches - Dry contact switches and tape is probably the most common type 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.
- 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 information security strategy.
- Identification Badge: Special identification badge such as employee cards, privileged access pass, and visitor passes etc. enable tracking movement of personnel. This may also be a card with signature and or photo identity. Security staff to permit or deny access and to detect unauthorized access physically examines identification badges.
- Manual Logging: All visitors to the premises are prompted to sign a visitor's register recording the date and time of entry and exit, name of entrant, organization, purpose etc. The visitor may also be required to authenticate his identity by means of a business card, photo identification card, driver's license etc.
- Electronic Logging: Electronic card users may be used to record the date and time of entry and exit of the cardholder 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. This security mechanism can be made with electronic or biometric devices.

- Controlled Single Point Access: Physical access to the facility is granted through a single guarded entry point. This involves identifying and eliminating or disabling entry from all entry points except one. Multiple entry points may dilute administration of effective security.
- Controlled Visitor Access: A pre-designated responsible employee or security staff escorts all visitors such as maintenance personnel, contract workers, vendors, and consultants for a specified time period (unless they are for long-term, in that case guest access may be provided).
- Bonded Personnel: This is useful in situation where physical access to sensitive facilities is given to employees or the contract employees. Bonding (contractors or employees being required to execute a financial bond), such bond does not improve security but reduces financial impact due to improper access/misuse of information resources.
- 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 access.
- Alarm Systems/Motion Detectors. Alarm systems provide detective controls and highlight security breaches to prohibited areas such as access to areas beyond restricted hours, violation of direction of movement. For example, in specific areas, entry only or 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.
- Secured Distribution Carts: One of the concerns in batch output control is to get the printed hardcopy reports (which may include confidential materials) securely by the intended recipients. In such cases, distribution trolleys with fixed containers secured by locks are used. The respective user team holds the keys of the relevant container.
- Cable Locks: A cable lock consists of a plastic-covered steel cable that chain a PC, laptop or peripherals to the desk or other immovable objects.
- 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.
- Switch Controls: A switch control is a cover for the on/off switch, which prevents a user from switching on or off the power.
- Peripheral Switch Controls: These types of controls are lockable switches that prevent a device such as a keyboard from being used.

- 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 physiological features of the user.
- Laptops Security: Securing laptops and portables represent a significant challenge, especially since; loss of laptops creates loss of confidentiality, integrity and availability. Cable locks, biometric mice/fingerprint/iris recognition and encryption of the data is some of the means available to protect laptops and data therein.

3.4.6 Smart Cards

A smart card used for access control is of 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 and can also provide information about the date and time of entry.
- Wireless Proximity Readers: A proximity reader does not require the user to physically insert the access card. The card reader senses the card in possession of a user in the general area (proximity) and enables access.

3.5 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.

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

- Tour of organizational 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 authorization, special access authorization, 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 organization.
- Examination of physical access logs and reports includes examination of incident reporting logs and problem resolution reports.

3.6 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 affect confidentiality, integrity and availability of the information, due to undesired changes in the environment or ineffective environmental controls.

3.7 Objectives of Environmental Controls

The objects of environment controls are the same as discussed in the section on physical controls. However, from the perspective of environmental exposures and controls, information systems resources may be categorized as follows:

- Hardware and Media
- Information Systems Supporting Infrastructure or Facilities
- Documentation
- Supplies
- People

3.8 Environmental Threats and Exposures

Exposures from environmental threats may lead to total or partial loss of computing facilities, equipment, documentation and supplies causing loss or damage to organizational data and information and more importantly people. It may significantly and adversely impact the availability, integrity and confidentiality of information. The threats can be broadly classified as Natural and Man-made.

3.8.1 Natural Threats and Exposure

- Natural disasters such as earthquakes, floods, 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
- Pandemic due to virus etc.

3.8.2 Man-made Threats Exposure

- Fire due to negligence and human action
- Threats from terrorist activities

- Power – uncontrolled/unconditioned power, blackout, transient, 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

3.9 Techniques of Environmental Controls

The IS supporting infrastructure and facilities should provide the conducive environment for the effective and efficient functioning of the information processing facility (IPF). Based on the risk assessment, computing equipment, supporting equipment, supplies, documentation and facilities should be appropriately protected to reduce level of risks from environmental threats and hazards or exposures. Following are list of controls, which are to be implemented.

3.9.1 Choosing and Designing a Safe Site

- Natural disasters. Natural disasters can include weather-related problems (wind, snow, flooding, and so forth) and earthquake may adversely impact the IPF. While establishing IPF, organization should consider issues related to probability of natural disaster.
- 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.

3.9.2 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:

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.

- 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 nonabrasive, and they should be protected to minimize 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.
- 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.
- 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.
- Media protection: Location of media libraries, fireproof cabinets, kind of media used (fungi resistant, heat resistant).

3.9.3 Emergency Plan

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

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 organization.

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.

3.9.4 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. Environmental controls should be documented and a suitable preventive maintenance should be put in place administered through schedules and logs.

- MTBF and MTTR: Failure modes of each utility, risks of utility failure, should be identified, parameterized and documented. This includes estimating the MTBF (Mean Time between Failures) and MTTR (Mean Time to Repair). 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. It is better that MTBF should be high and MTTR should be low.

3.9.5 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 damage of internal components. Air conditioning 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.

3.9.6 Power Supplies

Power supply should conform to computing equipment manufacturer specifications. Many aspects may threaten power system, the most common being noise and voltage fluctuations. Noise in power systems refers to the presence of electrical radiation in the system. 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:

- Uninterruptible power supply (UPS)/generator: UPS usually consist of battery backup or diesel generator that interfaces with the external power supplied to the equipment. On interruption in external power supply, the power continues to supply from the battery. 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, but for computerized environment, on-line UPS is mandated.

- 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.
- 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.

3.9.7 Fire Detection and Suppression System

Smoke 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.

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 organization.

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.

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.

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 at places like chemical laboratories and rarely occur 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 Water based systems and Gas based systems.

(a) Water Based Systems

Wet pipe sprinklers: In this case, sprinklers are provided 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 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 these, 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, 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_2 thus effectively cutting of oxygen supply from the air, which is a critical component for combustion. However, CO_2 being potentially lethal for human life, such systems are recommended only in unmanned computer facilities or in portable or hand-held fire extinguishers.

FM200: 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.

3.10 Auditing 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 they are 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.
- 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.

3.11 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

vulnerabilities the assets are exposed to. These threats could include unauthorized access to the resources, vandalism, and public disclosure of confidential information. The main source of threats is from outside people and the employees of the organization. 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.

3.12 Questions

1. Which of the following is first action when a fire detection system raises the alarm?
   A. Turn off the air conditioner
   B. Determine type of fire
   C. Evacuate the facility
   D. Turn off power supply
2. Which of the following are 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 dead man door, turnstile, mantrap is to:
   A. Prevent unauthorized entry
   B. Detect perpetrators
   C. Meet compliance requirement
   D. Reduce cost of guard
4. Which of the following is the 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 unauthorized persons
5. Which of the following is a 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 open doors based on access cards, pins, and/or biometric devices and are powered by electricity. Which of the following is the 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 center which of the site is best to be selected?

A. On topmost floor to delay the unauthorized visitor to reach

B. In the basement not easily accessible to perpetrator

C. On ground floor so that users can access it 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 center?

    A. Unauthorized changes and access in configuration

    B. Prevent photography of data center layout

    C. User can provide information to attacker on phone

    D. Mobile devices generate wireless communication

3.13 Answers and Explanations

1. C is the correct answer. Life safety takes precedence. Although other answers are important steps human life always is a priority.

2. A is the correct answer. Unmanned data center 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 is the correct answer. Primary purpose of all types of physical access control is to prevent unauthorized entry. Other objectives are secondary.

4. A is the correct answer. Human guard makes decisions and can address visitor's requirement and direct them appropriately. Others are supplementary functions.

5. B is the correct answer. False positive is a concern in biometric access security as it results in unauthorized access. Other option does not result in unauthorized access.

6. D is the correct answer. 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 is the correct answer. 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 is the correct answer. 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 is the correct answer. Top floor and basement have risk of seepage and flooding. Ground floor has risk of easy attack.

10. A is the correct answer. Mobile devices can be connected to servers, resulting in unauthorized changes. Other concerns are secondary.

Chapter 4

Logical Access Controls

4.1 Introduction

Today information systems store and process a wide variety of data in centrally hosted 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. Information that is residing on a system and accessed by many users has an associated risk of unauthorized access. Logical access controls are a means of addressing concerns associated with unauthorized accesses. Logical access controls are protection mechanisms that limit users' access to data and restrict their access on the system.

4.2 Objectives of Logical Access Controls

The objective of logical access controls is to ensure that authorized 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 it should be just sufficient for one to perform one’s duty without any problem or restraint. Logical access controls are all about protection of information assets in all three states, namely: rest, in transit and at process.

4.3 Paths of Logical Access

An IS auditor has to identify and document the possible logical access paths permitting access to information resources, which may involve testing security at various systems viz. hardware, system software, database management system, application software, access control software. Each of these routes has to be subjected to appropriate controls in order to secure it from the possible logical access exposures.

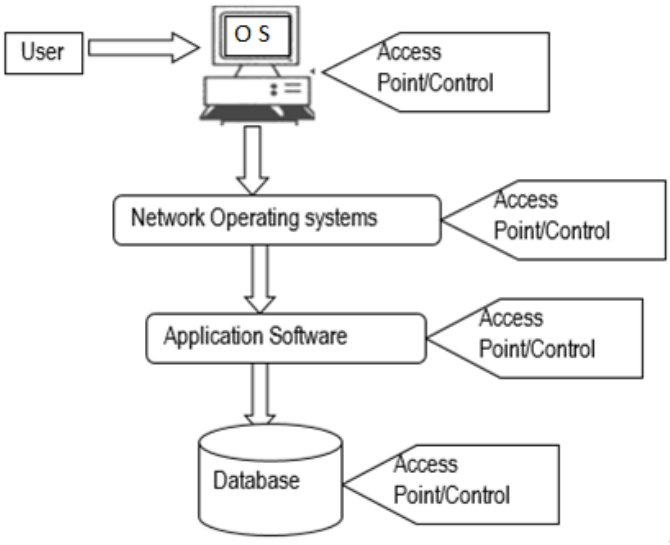


Fig. 4.1: Paths of Logical Access

4.4 Logical Access Attacks and Exposures

Improper logical access can result in loss or damage to information and resources leading to undesirable consequences for an organization. It can also result in violation of the confidentiality or integrity or availability of information. There are various types of exposures related to logical access controls; some of the technical attacks are discussed below:

- Masquerading: It is a means of disguising or impersonation. The attacker pretends to be an authorized user of a system in order to gain access to or to gain greater privileges than they are authorized for. A masquerade may be attempted using stolen logon IDs and passwords, through finding security gaps in programs, or bypassing the authentication mechanism. The attempt may come from within the organization such as, from an employee or from an outside user through some connection from the public network. Weak authentication provides one of the easiest ways for a masquerade. Once the attacker has logged in, they may have full access to the organization'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.
- Piggybacking: Unauthorized access to information by using a terminal that is already logged on with an authorized ID (identification) and left unattended.
- Wiretapping: Tapping a communication cable to collect information being transmitted.

- Denial of Service: One way of denial of service is to choke the bandwidth by connection flooding. The perpetrator attempts to send multiple sessions requests, resulting in non-availability of sessions for legitimate users.
- 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 revealing confidential information like user ID, Password, PIN and any such information required for login as authorized user. Social engineering attack may result into physical or logical attacks.
- Phishing: User receives a mail requesting to provide authentication information by clicking on embedded link. The mail and link appear to be actual originator e.g. Bank. Ignorant users click on the link and provide confidential information. The most popular attacks on banking systems in the recent times, they target innocent users, using a combination of social engineering, e-mail and fake websites to con the user to click on a link embedded in an apparently authentic mail from a reputed bank. The link takes the users (generally a customer of the bank) to a look-alike Bank website that gets the personal details of the user including details such as PIN and Internet banking password, which is then exploited by the hacker.
- Vishing: Uses the similar technique over telephone.
- Key Logger: Perpetrator installs software that captures the key sequence used by the user including login information. Key logger can be sent thru mail or infected pen drive. There are hardware key loggers available that are connected to system where keyboard is attached.
- Malware: Specially designed programs that captures and transmits the information from compromised system. Malicious software (also called “Malware”) intentionally causes disruption and harm or circumvent or subvert the existing system’s function. Examples of malware include viruses, worms, trojan Horses, and logic bombs. Newer malicious code is based on Active X and Java applets.

4.5 Access Control Mechanism

The primary function of logical access control is to allow authorized access and prevent unauthorized access. Access control mechanism is actually a three-step process as depicted in the figure below:

- Identification: Identification is a process by which a user provides a claimed identity to the system such as an account number.
- Authentication: Authentication is a mechanism through which the user’s claim is verified by the system.

- 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 authorized access and prevent unauthorized access to information resources in an organization. Therefore, it may become necessary to apply access control at each layer of an organization'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 authorization and logging and reporting of user activities. Interfaces exist between operating system access control software and other system software access control programs such as those of routers, firewalls etc. that manage and control access from outside or within organization networks. On the other side, operating system access control software may interface with databases and / or application system access controls to application data.

4.5.1 Identification Techniques

Implementing the right process of confirming the identity is a challenge. Authentication is the process of verifying that the identity claimed by the user is actually true or false. Users are authenticated using one of three authentication factors or techniques. The three categories of authentication factors are:

- 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)

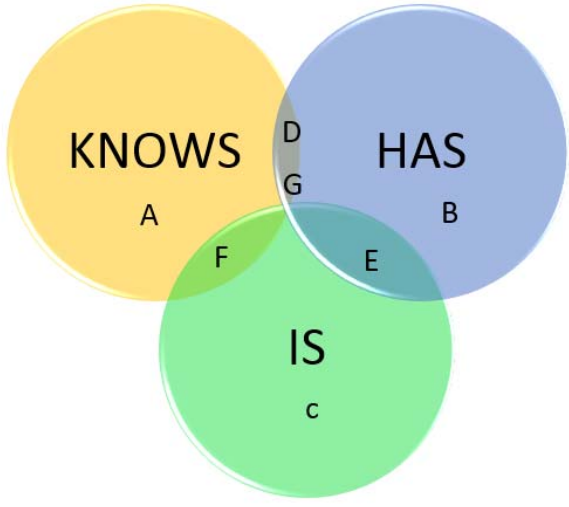


Fig. 4.2: Multi-factor Authentication

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

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 strength 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 and can be held accountable for any actions taken. A default denial 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 information owner.

4.5.2 Authentication Techniques

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

Fig. 4.3: What you have (Token), what you know (password/PIN) and who you are (Physiological features)

4.5.2.1 Passwords and PINs

- Password: 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 match and is successful for both fields, the system authenticates the user and enables access to resources based on the access control matrix. However, if a match is not successful, the system returns a message (such as “Invalid User-id or password”), 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 randomly generated such that a person or a computer cannot guess it in sufficient time and attempt by using a guess and check method. PINs are commonly used for gaining access to Automated Teller Machines (ATMs).

4.5.2.2 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 100 seconds 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, and so it is more secure.

4.5.2.3 Challenge Response System

An alternative to one-time passwords is challenge response system. Instead of having the device just blindly generating 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 sends that output to the server. This scheme is slightly more complicated, but it allows the password to be based on changing input rather than just time.

4.5.2.4 Passphrase

A passphrase is a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security. Passphrases are often used to control both access to, and operation of, cryptographic programs and systems, especially those that derive an encryption key from a passphrase. Passphrases are stronger than passwords because of:

- They usually are (and always should be) much longer—20 to 30 characters or more is typical—making some kinds of brute force attacks entirely impractical.

- If well chosen, they will not be found in any phrase or quote dictionary, so such dictionary attacks will be almost impossible.
- They can be structured to be more easily memorable than passwords without being written down, reducing the risk of hardcopy theft.

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
- 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.

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.
- System should be configured to must change password on first login.
- System should be configured to force password change periodically e.g. once in 60 days.
- System should be configured for minimum age of the password.
- Concurrent logins 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 stored in an encrypted form using one-way encryption.
- System should be configured for password history control; e.g. System will not accept last five passwords

Attacks on Logon/Password Systems

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

- Brute Force: It is a form of attack, wherein attacker tries out every possible technique to hit on the successful match. The attacker may also use various password cracking software tools that assist in this effort.
- Dictionary Attack: It is based on the assumption that users tend to use common words as passwords, which can be found in a dictionary.
- Trojan: it is 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 program, 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 unauthorized user may wait for an authorized user to log in and leave a terminal unattended. This can be controlled by automatically logging out from the session after a pre-determined period of inactivity or by using password-protected screen savers.

4.5.2.5 Token Based Authentication

Objects that a user is required to possess for identification and authentication are known as tokens. In general, tokens are of two type:

- Memory tokens: It is most common form of tokens; the cards contain visible information such as name, identification number, photograph and such other information about the user and a magnetic strip or memory chip. This magnetic strip or memory chip 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/memory token and passes onto the computer for verification of the 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.
- 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. In general, smart tokens are processor based and contain a processor chip. Smart tokens are capable of processing data within their chip.

4.5.2.6 Biometric Authentication

Biometrics offers authentication based on "what the user is". Biometrics are automated mechanism, which uses physiological and behavioural characteristics to determine or verify identity. 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. Some of the biometric characteristics, which are used, are:

- Fingerprint
- Facial Scan
- Hand Geometry
- Signature
- Voice
- Keystroke Dynamics
- Iris Scanners
- Retina Scanners

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 unauthorized 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 tend to inversely related. An overall metric used is the Equal Error Rate (EER), which is the point at which FRR equals FAR. Finger print-based biometric controls are quite popular and widely deployed in data centres.

4.5.3 Authorization 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. 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
    - Password Policy
    - Account Lockout Policy
- Manage audit policy
- Log events and report capabilities

Pluggable Authentication Modules

- The pluggable authentication module (PAM) framework provides system administrators with the ability to incorporate multiple authentication mechanisms into an existing system using 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

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 at also may have access to the file. Again, most operating systems have at least three types of file permissions; read, write and execute (execute permission is only for executable programs and not every file). The users have to be given at least read access to many of the system files.

Access Control Lists (ACL)

An access control list is a table that tells, 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). Following table is an example of access control list:

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

4.6 Logical Access Control Techniques

4.6.1 Logical Access Controls Policy and Procedures

Logical 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. Logical access control policy typically covers the following:

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

4.6.1.1 User Management

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

- User registration
- Privilege user 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 confirmed by User manager. Information owner must approve this. User registration process should answer:

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

4.6.1.2 Privilege User Management

Access privileges are to be aligned with job requirements and responsibilities. The job requirements 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/modify 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 should be part of process. Many times, application or database privilege management does not provide for automatic revocation of such accesses. In such cases, manual monitoring and periodic reviews are compensating controls to correct the situation.

4.6.1.3 Default Users Management

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. Many-a-times there are multiple default users in the products. The user ID and Passwords for these default users are published by the vendor in their user/system manuals. It is expected that these default users' names and passwords must be changed as soon as system is implemented. While reviewing logical access controls, IS auditor must ensure that default user-ids are either disabled, or their passwords have been changed and suitably controlled by the organization.

4.6.1.4 Password Management

Password management should be taken care of, based on the password policy. Following are some of the Password management functions:

- Allocations of password which is generally done by system administrators
- Secure communication of password to the user
- Force change on first login by the user so as to prevent possible misuse by system administrators
- Storage of password should not be done in clear text. Most of the systems store passwords as hash value of the password.

- During authentication process, passwords should be transmitted by generating hash and should be 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. Users' account should be locked after predefined number of unsuccessful login attempts.
- Reissue password after confirming the identity of users, in case of expired passwords 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.

4.6.1.5 User Access Rights Management

Following are some of the aspects with respect to user access rights management:

- Periodic review of user's access rights is essential process to detect possible excess rights due to change in responsibilities, emergencies, and other changes.
- Information owner must conduct periodic review of the access rights.
- There should be predefined period of account lifetime, after which user re-registration process should be started.
- Multiple login sessions should not be permitted.
- Wherever, there is possibility of conflict of interest, access controls should be automated.

4.6.2 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, intranet and Internet access. There are various tools and techniques used to manage these accesses. Network based tools and techniques like protocol control, service monitoring is discussed in network security chapter.

- Policy on use of network services: An enterprise should have a policy that specifies the use on Internet and Internet based services while using organization's devices.
- Segregation of networks: An enterprise should have segregation of networks, depending upon the sensitivity of business function applications.
- Network connection and routing control: The traffic between networks should be controlled, based on identification of source and authentication across the enterprise 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.
- Clock synchronization: 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 organization. In modern networks, this function is centralized and automated. This may also be useful in case of legal dispute.

4.6.3 Application Access Controls

Applications are most common assets that accesses information. Users invoke the programs/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.

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

- Sensitive system isolation: Based on the criticality of an application system in an enterprise, it may even be necessary to run the system in an isolated environment. This may be implemented through creating multiple DMZs. For example, Internet Banking application is kept in separate DMZ. (DMZ – Demilitarised Zone)
- Event logging: In application 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 applications 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.

4.6.4 Database Access Controls

Database access control is a method of allowing access to company's sensitive data only to those people (database users) who are allowed to access such data and to restrict access to unauthorized persons. In DBMS environment, DBA has typically access to the entire database

he/she administers. To address this problem, solutions have been proposed including the segregation of DBAs from user data, as in the case of the Oracle Database Vault product, and techniques for joint administration of critical database objects.

Oracle Database Vault restricts access to specific areas in an Oracle database from any user, including users who have administrative access. For example, company can restrict administrative access to employee salaries, customer medical records, or other sensitive information. This enables company to apply fine-grained access control to its' sensitive data in a variety of ways. It hardens company's Oracle Database instance and enforces industry standard best practices in terms of separating duties from traditionally powerful users. Most importantly, it protects the data from super-privileged users but still allows them to maintain the Oracle databases. Oracle Database Vault is an integral component of the enterprise.

4.6.5 Operating System Access Control

Operating system provides the platform for an application to use various information system resources and performs the specific business function. 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 should provide appropriate controls, which could prevent misuse by an intruder.
- User identification and authentication: The users must be identified and authenticated in a defined manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means such as Digital Certificates should be employed.
- Password management system: An operating system could enforce selection of good passwords. Internal storage of passwords should use one-way hashing algorithms and the password file should not be accessible to users.
- Use of system utilities: System utilities are the programs 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 administrator.
- Terminal/Session time out: Log out the user if the terminal is inactive for a defined period. This will prevent piggybacking.
- 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 pm and before 8.00 am or on a Saturday or Sunday.

4.7 Identity Management and Access Controls

Identity and access management (also called IDAM) is a framework of policies and technologies for ensuring that proper people in an enterprise have the appropriate access to technology resources.

The task of IDAM is controlling the user access provisioning lifecycle on Information Systems. It maintains the identity of a use and 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.

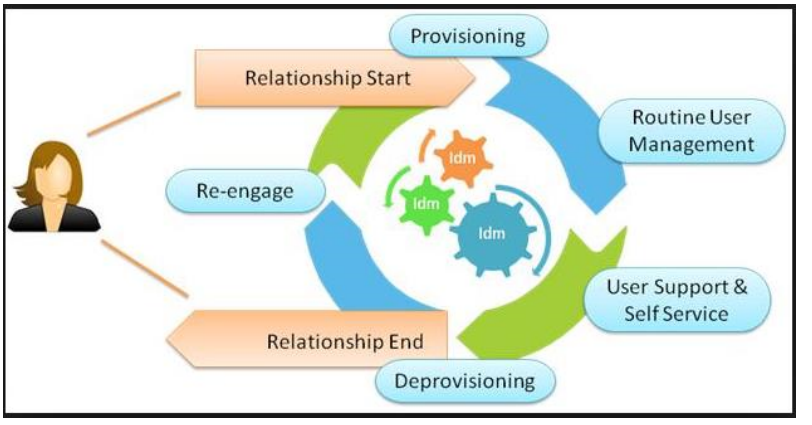


Fig. 4.4: Components of identity management

The core objective of an IDAM system is setting one identity per individual. Therefore, IDAM system provides administrators the tools and technologies to enforce logical access control policies on an ongoing basis across an entire enterprise and to ensure compliance with corporate policies, legal and regulatory requirements.

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 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.

4.8 Single Sign-On (SSO)

Single Sign-On addresses the practical challenge of logging on multiple times to access different resource. In SSO, a user provides one ID and password per work session and is automatically logged on to all the required applications.

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. Some of the common implementation of SSO is as under:

1. Active Directory (AD)

AD is a directory service implemented by Microsoft for Windows domain networks. An AD domain controller authenticates and authorizes 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 credential to determine 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. 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. 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)

2. Kerberos

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.

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. If one password is compromised, the attacker can have access to all privileges of users whose password is compromised.
- It is difficult to implement when organization has legacy applications or applications that cannot be plugged in with SSO.
- Maintaining SSO is tedious and prone to human errors.

4.9 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*** (passive) 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 controls:

- Mandatory access control: It is a multi-level secure access control mechanism. It defines a hierarchy of levels of security. A security policy defines mandatory access control.
- 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. Access control lists are used to store the rights with object.
- Role based access control: In some environments, it is problematical to determine the ownership of resources. In role-based systems, users are assigned roles based on their job functions in the information system environment. These systems are centrally administered and are nondiscretionary in nature.

4.10 Audit Trail

Primary objective of audit trail is to fix accountability to individual user for the activities performed by them. Generating and reviewing activity logs can do this. However, many times, IT persons are reluctant to enable logs since logs are resource consuming. It requires additional storage, separate access controls, and in some cases programming efforts. The issue can be resolved by defining priorities based on risk assessment results and logs for required 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 activities generated by the system that enables the reconstruction and examination

of the sequence of events of a transaction, from its inception to output of results. Violation reports present significant, security-oriented events that may indicate either actual or attempted policy transgressions reflected in the audit trail. Information owner to identify any unauthorized change or access should regularly review violation reports. 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 information. An audit of information system security searches for the following:

- Internal and external attempts to gain unauthorized access to a system
- Patterns and history of accesses
- Unauthorized 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. 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, the integrity of the audit logs should be maintained.

4.11 Auditing Logical Access Controls

Following are some of factors critical while evaluating logical access controls:

- Understanding of an organization's information security framework
- Selection and implementation of appropriate access controls
- Top management's commitment
- Management controls
- Explicit access permission to information or systems
- Periodic review / audit of access permission

Audit Test Procedures

IS Auditor should:

- Evaluate whether logical access policies and standards exist and are effectively communicated and implemented.
- Interview information owners, users and custodians to evaluate their knowledge and skills on implementation of logical access controls.
- Evaluate the existence and implementation of procedures and mechanisms for logical access to ensure protection of organizational information assets.

- Evaluate the various logical security techniques and mechanisms for their effective implementation, operation and administration.
- Test the effectiveness and efficiency of logical access controls
- Test the appropriateness of system configuration and parameter settings.
- Test the compliance of system configuration with the organizational information security policy, standards and manufacturer baseline security requirements.
- Test the existence and implementation of process of authorization for configuration of access security settings and parameters and changes thereto.
- Evaluate and review the documentation of controls over privileged and special purpose logons
- Evaluate the existence of 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.
- Verify the control of authorization, operation and termination over use of tokens such as memory and smart cards.
- Verify the 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.
- Verify the security practices relating to unattended terminals, security of data in transit and control over production resources.
- Verify the logging of transactions and events.
- Evaluate mechanisms for vulnerability analysis in s access control features and software
- Evaluate the effectiveness of user management procedures
- Test user profiles and group profiles to determine the access privileges and controls thereon.
- Review audit trails, access violation reports in respect of all privileged logons and special user accounts
- Review the adequacy of process for monitoring and incident handling procedures
- Review the control over systems files and directories containing critical hardware and systems software configuration and parameter files such as driver information, etc.
- Review the control over application files and directories containing application programs, support files, program libraries, parameter files, initialization files, etc.

- Evaluate the control over production data and directories containing production files and production resources.
- Verify whether bypassing of security procedures is being done, if any.

4.12 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 and vulnerabilities. Most important consideration is identifying users, type of access, and the asset. It is best to adopt a least privilege policy on the basis of "need to know, need to do". Auditor should know that access control defines how users should be identified, authenticated, and authorized. This is generally addressed in information security policies and procedures, hence the starting point of audit of logical access controls should be to understand the policies and procedures and ensure that these are implemented uniformly across the organization.

4.13 Questions

1. Which of the following pair of authentications can be considered as two factors?
   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. Authorization
   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 information 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 unauthorized or excess accesses to users?
   A. Identification
   B. Authentication
   C. Authorization
   D. Review
7. While auditing compliance with password policy, IS auditor observed that configuration of password parameters in system is as per information security 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 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. Authorize users based on role
   D. Compliance with policy

4.14 Answers and Explanations

1. D is correct answer. The three factors are what a user knows (PIN, Password, and Passphrase), what user possesses (Access card, Token) and what unique characteristics of user (Biometric). Use of any two factors for authentication is called two factors. Option A, B and C use only one factor.
2. A is correct answer. Identification of user is first and primary requirement of granting access. Next will be authentication method to be established and finally finding authorization levels based on role that also addresses need to know.
3. B is correct answer. Mandatory accesses are those controls that are to be applied uniformly across organization and are defined by information security policy. D is discretionary access controls. B and C generally do not specify such requirements.
4. C is correct answer. Single point of failure is a major concern. One password if compromised, all accesses for that user are available to perpetrator.
5. B is correct answer. Password sharing by user is most difficult to get evidence for or detect. Others can be monitored or enforced using technology.
6. D is correct answer. 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, emergency, resignation and retiring of employees. In such situations sometimes revocation of accesses is missed out, which can be corrected during review.
7. C is correct answer. Review of log for password configuration may disclose the compliance of policy because policy is configured in the system through password

configuration. This may also detect unwarranted changes made by a malicious user (who obtains administrative access) in the password configuration. However, option A and D may provide assurance for compliance of password policy configurations in the system, not the policy itself. Option D is not relevant.

8. A is correct answer. Strength of one-time password is that it is active for short time, if user does not login during that time the one-time password expires. One-time password is unique for each session and user; however, it is not a strength. It can be communicated by suitable means.

9. D is correct answer. In Social engineering attacks, the weakest link is unsuspecting human user. Attacker uses techniques to compel users to reveal passwords and other confidential information. For example, in Phishing. Other options are technology-based attacks and can be detected or controlled.

10. C is correct answer. Primary objective of implementing access controls is to restrict access to authorized people. Fixing accountability of actions is the primary objective of audit trail. Others are means to implement access controls not objectives.

Chapter 5
Network Security Controls

5.1 Introduction

We have seen the use of networks for business communication and application hosting in e-learning, in this section, we will review the risks and controls that are specific to networked environment. Now-a-days, real life organizations are using large and complex network infrastructure. Hence, 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 having focus of attacker. Therefore networks are also far more vulnerable to external and internal threats.

Organization 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 information assets) are applicable to network security. In addition one needs to look at network specific controls to ensure that organization's information security objectives are achieved.

5.2 Objective of Network Security Controls

There is threat of interception of information when it travels on intranet or Internet. Malicious users, hackers, adversaries may try to gain unauthorized access to organization's data or information. Non-availability of information assets to interested parties may also adversely impact the organization. There are three main objectives of network security controls.

- Confidentiality: Maintaining the confidentiality and privacy of information and information assets when it travels on the network. Interception may be a concern to this.
- Integrity: Ensuring the correctness and completeness of data or information traversing the network. There may be attempt to tamper data in-transit or data stored on information systems by exploiting the vulnerabilities of network devices or channels. Unauthorized manipulation of data during transit may question the integrity of the data.
- Availability: Keeping the information and network resources available to the authorised stakeholders. Denial of service or distributed denial of service is a major threat to the availability of information.

5.3 Network 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. 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. 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

Information Gathering

A serious attacker will spend a lot of time obtaining as much information as s/he may have 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 program 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 organization 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.
- 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. 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: 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.

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 unauthorized use of a network connection, or a theft of service.
- Optical fiber: It is not possible to tap an optical system without detection. Further optical fiber carries light energy, not electricity, which does not emanate a magnetic field as electricity does. Therefore, an inductive tap is impossible on an optical fiber cable. However, the repeaters, splices, and taps along a cable are places at which data may be intercepted more easily than in the fiber 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.

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.

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 unauthorized 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.

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.

- Mis-delivery: Message mis-delivery happens mainly due to congestion at network elements which causes buffers to overflow and packets dropped. Sometimes messages

are mis- delivered 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.

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

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.

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.

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.

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.

5.4 Current Trends in Attacks

Most attacks and threats discussed above are being in use for a considerable time. Organizations 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 systems. Some of these are discussed below.

Exploiting Application Vulnerabilities

With use of internet based technologies and clouds, organizations have hosted applications that can be accessed from internet and/or intranet. These applications might contain vulnerabilities and if exploited can compromise security of information. Attackers try to exploit these vulnerabilities to launch the attacks, like SQL Injection, Cross site scripting etc. OWASP (Open Web Application Security Project) identifies top ten security threats every year. Threats identified in 2017(This is latest at the time of writing this material) are listed below. (Source: www.owasp.org)

- Injection: Injection flaws, such as SQL, NoSQL, 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: Application functions related to authentication and session management is often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
- Sensitive data exposure: Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
- XML external entities (XXE): Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
- Broken access control: Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
- Security misconfiguration: Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but also, they must be patched/upgraded in a timely fashion.
- Cross-site XSS: XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. 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 deserialization: Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

- Using components with known vulnerabilities: Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
- Insufficient logging & monitoring: Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Advanced Persistent Threat (APT)

A sustained targeted attack on identified subject, which remains undetected for a prolonged time period. Attacker tries to introduce malware to compromise the system. For this, attacker uses possible social engineering methods. Once the system is compromised the malware resides in the 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 the attacked system to the 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 organization is received by the attacker or as long as the attack is undetected.

5.5 Network Security Controls Mechanism

This section examines controls available to ensure network security from the various identified threats and vulnerabilities.

5.5.1 Network Architecture

The architecture or design of a network may 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 isolates network, thereby, giving better control. 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. (Figure 5.1).
- 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 be to have two servers, using a “failover mode”. In failover mode, the

servers communicate with each other periodically, determining if the other is still active. If one fails, the other takes over processing.

- 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.

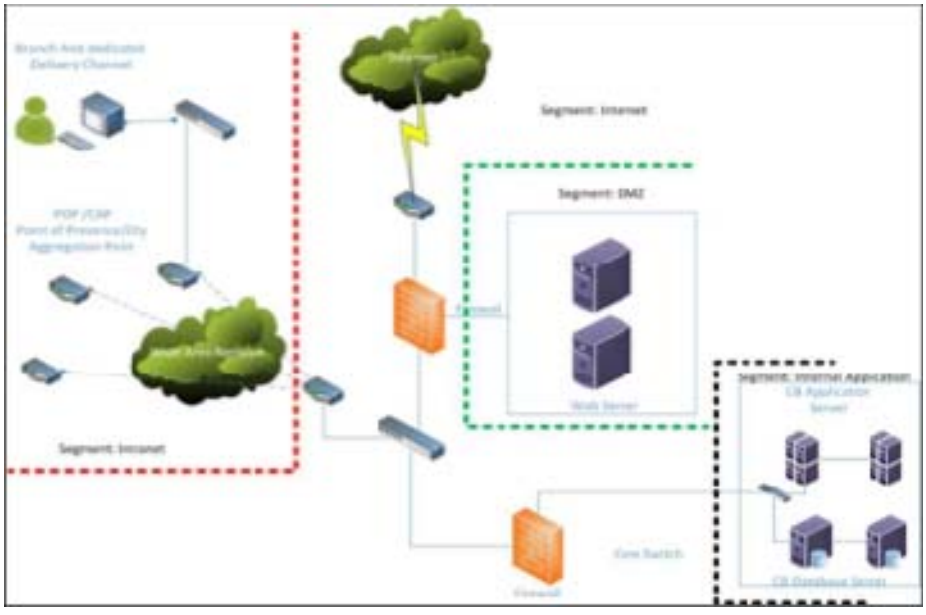
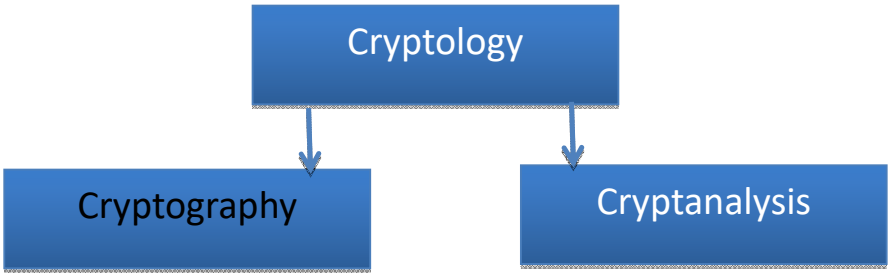


Fig. 5.1: Segmented Architecture

5.5.2 Cryptography

Cryptography is a branch of cryptology. It is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing." There are two essential elements of cryptography, one is algorithm and the other is key.

Cryptanalysis: The goal of cryptanalysis is to find some weakness or insecurity in a cryptographic scheme, thus permitting its subversion or evasion.



5.5.2.1 Types of Cryptography

Mainly, the types of cryptography depend upon the algorithm used for encrypting and decrypting a message. There are three types of cryptographies.

- Secret-key cryptography or symmetric-key cryptography
- Public key Cryptography or Asymmetric key cryptography
- Hash Function or message digest
- Symmetric key cryptography (or symmetric encryption) uses same key to encrypt and decrypt the messages. Such a method of encrypting information has been largely used in the past decades and it is still in use to facilitate secret communication between governments and defence establishments. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. Symmetric key ciphers or algorithms are implemented as either block ciphers or stream ciphers. A block cipher encrypts input in blocks of plaintext as opposed to individual characters that is used by a stream cipher. A significant disadvantage of symmetric ciphers is the key management necessary to distribute them securely.
- Asymmetric or public key cryptography: Asymmetric cryptography, also known as public key cryptography, uses private key and public key pair to encrypt and decrypt messages. The keys are simply large prime numbers that have been paired together mathematically but are not identical (asymmetric). One key of the pair can be shared with everyone; it is called the public key and the other should be ket secret, which is private key. Under this system a pair of keys is used to encrypt and decrypt messages. A public key is used for encryption and a private key is used for decryption. A private key is used to establish non-repudiation. Public key and Private Key are unique key pair but different.
- Hash function: A hash function is a one way and used to map data of arbitrary size to fixed-size values. The values returned by a hash function are called hash values, hash codes, message digests, cryptographic checksum or simply hashes. Hash function has three characteristics:

- It is one-way encryption.
- It gives message digest or hash value of fixed length. Length of massage digest or hash value depends upon hashing algorithm.
- It is always unique to the text. Any change in the text, results in changing the message digest or hash value dynamically.

Examples of hashing algorithms are MD5, SHA1, SHA2, SHA3 (Secured Hashing Algorithm) etc.

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.

5.5.2.2. Public Key Infrastructure (PKI)

- A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.
- Public-key cryptography uses a key pair to encrypt and decrypt content. The key pair consists of one public and one private key that are mathematically related. Public keys , which may be disseminated widely, and private keys which are known only to the owner of the digital certificate.

Components of PKI

Digital Certificates: A Digital Certificate is a digitally signed document that associates a public key with a individual or web site. The certificate can be used to verify that a public key belongs to an individual or web site. In a typical public key infrastructure (PKI) scheme, the signature will be of a certifying/ certification authority (CA). The signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.

In general it is issued by certifying authorities. However, private digital certificates may also be generated. Private digital certificates are not acceptable by the legal systems.

Types of digital certificates:

- Digital Signing Certificate: Issued to the Individuals
- Digital Encryption Certificate: Issued to individuals or servers
- Code Signer (Software code)

Contents of a Typical Digital Certificate

- Serial number: Used to uniquely identify the certificate.
- Subject: The person or entity identified.
- Signature: The algorithm used to create the signature.
- Issuer: The entity that verified the information and issued the certificate.
- Valid-from: The date from which the certificate is valid.
- Valid-to: The expiration date.
- Public key: The public key to encrypt a message to the named subject.
- Thumbprint algorithm: The algorithm used to hash the certificate.
- Thumbprint: The hash itself to ensure that the certificate has not been tampered with.

Digital Signatures

- It is signed message digest or hash value of the document. With digital certificate, message digest or hash value of the digital documents are signed and digital signature is affixed to the documents. Private key is used for generating the digital signature.
- Digital Signature is a process that guarantees that the contents of a message have not been altered in transit. When you, the server, digitally sign a document, you add a one-way hash (encryption) of the message content using your private key.

Controller of Certifying Authority

- The Controller of Certifying Authorities (CCA) has been appointed by the Central Government under section 17 of the Act for purposes of the IT Act. The Office of the CCA came into existence on November 1, 2000. It aims at promoting the growth of E-Commerce and E- Governance through the wide use of digital signatures.
- The Controller of Certifying Authorities (CCA) has established the Root Certifying Authority (RCAI) of India under section 18(b) of the IT Act to digitally sign the public keys of Certifying Authorities (CA) in the country. The RCAI is operated as per the standards laid down under the Act.
- The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a licensed CA issues a given certificate. For this purpose it operates, the Root Certifying Authority of India(RCAI). The CCA also maintains the Repository of Digital Certificates, which contains all the certificates issued to the CAs in the country.

Certifying Authority (CA)

Certifying Authorities are Trusted Third Parties (TTP) to verify and vouch for the identities of entities in the electronic environment. The trust in the CA is the foundation of trust in the certificate as a valid credential. In India, the IT Act (Information Technology Act) provides for the Controller of Certifying Authorities (CCA), the body under Ministry of Electronics and Information Technology to license and regulate the working of Certifying Authorities and also to ensure that none of the provisions of the IT Act are violated.

Certificate Revocation List (CRL)

Certificate Revocation List (CRL) is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore entities presenting those certificates should no longer be trusted. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. The CRL file is itself signed by the CA to prevent tampering. The CA that issues the corresponding certificates always issues the CRL. When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user.

5.5.2.3 Quantum Cryptography

Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best-known example of quantum cryptography is quantum key distribution, which offers an information-theoretically secure solution to the key exchange problem. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or assumed to be impossible using only classical (i.e. non-quantum) communication. For example, it is impossible to copy data encoded in a quantum state. If one attempts to read the encoded data, the quantum state will be changed. This could be used to detect eavesdropping in quantum key distribution.

5.5.2.4 Application of Cryptographic Systems

In electronic transmissions it is essential to protect from threats relating to confidentiality, integrity, authentication and non-repudiation. A system is needed that protects against these security concerns. To address these security concerns, we have cryptographic systems like:

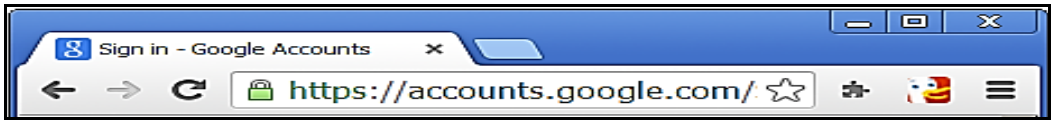
- Transport Layer Security
- IPsec
- SSH
- Secure Multipurpose Internet Mail Extension (SMIME)

Secure Socket Layer (SSL) / Transport Layer Security (TLS)

- The Secure Socket Layer (SSL) and Transport Layer Security (TLS) is the most widely deployed security protocol used today. SSL was first developed by Netscape and subsequently became Internet standard known as TLS (Transport Layer Security).The main differences between SSL and TLS are technical in terms of the generation of key material.
- SSL/TLS are essentially protocols that provide a secure channel between two machines operating over the Internet or an internal network. In today's Internet focused world, the SSL protocol is typically used when a web browser has to securely connect to a web server over the inherently insecure Internet. SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely.

Transport Layer Security (TLS)

1. Browser connects to a web server (website) secured with SSL. Browser requests that the server identify itself.
2. Server sends a copy of its SSL Certificate, including the server's public key.
3. Browser checks the certificate root against a list of trusted CAs and to verify that the certificate is not expired, not revoked, and that its common name is valid for the website that it is connecting to. If the browser trusts the certificate, it creates, encrypts, and sends back a symmetric session key, encrypted with the server's public key.
4. Server decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.
5. Server and Browser now encrypt all transmitted data with the session key.



Almost any service on the Internet can be protected with TLS. TLS is being used for

- Secure online credit card transactions.
- Secure system logins and any sensitive information exchanged online e.g. secure Internet Banking session
- Secure cloud-based computing platforms.
- Secure connection between E-mail Client and E-mail Server.

- Secure transfer of files over https and FTP(s) services.

Secure intranet based traffic such as internal networks, file sharing, extranets, and database connections.

Internet Protocol Security (IPSEC)

Virtual Private Network (VPN)

VPNs connect private networks through untrusted networks like the Internet; they establish a tunnel and use strong encryption to provide privacy and strong authentication to guarantee identity, so they are more secure than traditional networks. VPN provides confidentiality and integrity over insecure or untrusted intermediate networks. IPsec enables VPN and ensures secure communication.

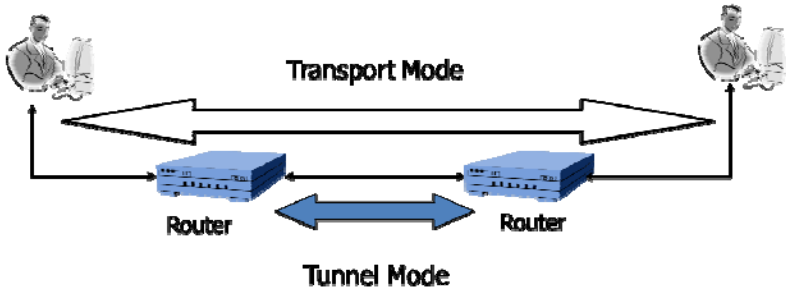
A virtual private network (VPN) is created by building a secure communications link between two nodes by emulating the properties of a point-to-point private link. A VPN can be used to facilitate secure remote access into a network, securely connect two networks together, or create a secure data tunnel 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.

IPsec

IPsec is encryption at IP (network layer); it protects any application data across IP Network. That is the reason applications need not be specifically designed for use of IPsec. IPsec is a framework for a set of protocols used for security. IPsec is useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. IPsec is implemented at end routers/firewalls or clients.

IPsec operates in two modes:

- Transport mode (for end-to-end) provides secure connection between two end points. In this mode data is encrypted but the header of the packet is not encrypted
- Tunnel mode (for VPN): With tunnel mode, the entire IP packet is encrypted and a new header is added to the packet for transmission through the VPN tunnel.



Secure Shell (SSH)

- SSH is usually used for UNIX systems and encrypts the commands getting transmitted. It works in a client-server mode and both ends of the client/server connections are authenticated using digital certificates.

Secure Multipurpose Internet Mail Extension (SMIME)

- S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data. Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email messages to support text in character sets other than ASCII, as well as attachments of audio, video, images, and application programs. Message bodies may consist of multiple parts, and header information may be specified in non-ASCII character sets.

5.5.3 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 maintaining 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 mobile computing
- Building more efficient ties with customers, suppliers, and employees

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 authorized lines or locations. When a user dials into the server and identifies itself, the server records the request and disconnects the call. Then server calls the user at a

pre-determined number and then enables the user to access the resources based on authentication. A weakness in this procedure is call forwarding. An unauthorized person could enable calls to a pre-determined number to be forwarded to the number designated by him, thus enabling him to gain unauthorized access to the resources.

Other Controls

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

Authentication Servers

In widely dispersed networked environment, it is crucial to accomplish user management and enabling authorized access to users including to mobile users. In such circumstances all access control is transferred to a centralized or decentralized access authentication mechanism. Two of the popular applications of remote authentication mechanisms depending on centralized/decentralized 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 centralized user management
- Facilitates centralized access monitoring and control
- Enables modification of users access permission centrally
- Provides event logging and extended audit trails

5.5.4 Malicious Code

Malicious code is the name used for any program 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 (program) 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, then affected areas are known as "infected".

Viruses often perform some type of harmful activity on infected hosts, such as consuming 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 programs which install themselves without the user's consent.

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

- Master boot record (MBR) viruses: Affects the boot sector of storage device and further infects when the storage is accessed.
- Stealth viruses: Stealth viruses hide themselves by tampering the operating system to fool antivirus software into thinking that everything is functioning normally.
- 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
- Macro viruses: Macro viruses are the most prevalent computer viruses and can easily infect many types of applications, such as Microsoft Excel and Word.
- 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 code. 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.

Worms

Worms are stand-alone viruses in that, they are transmitted independently and execute themselves.

Trojan Horse

It is a malicious code hidden under legitimate program, such as a game or simple utility. Attackers, to infect the system and then get control remotely, to make that system work for them, primarily use Trojans.

Malware Protection Mechanisms

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

Anti-virus: Antivirus is most common protection from virus. Most of the antivirus software utilizes a method known as signature detection to identify potential virus attack on a system. 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 try 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.

Incident handling: Incident Handling is an action plan for dealing with malware attack. In case of malware incidents it is most essential to find out root cause to stop the reoccurrence.

Training and awareness programs: Human resources are the weakest link in information security. Periodic training and awareness programs need to be organized to ensure that employees and other third party users are made aware of the risks arising out of malware attack. This covers:

- 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

5.5.5. Firewalls

The technical details of firewalls, their types and configurations have been dealt with in the e-learning. Only certain specialized 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 organizations 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 organization 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 organizations, 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 organizations 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. 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.
- 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.

5.5.6 Intrusion Detection Systems

An intrusion detection system (IDS) is a device, usually another separate device, which monitors activity to identify malicious or suspicious events. An IDS is a sensor that raises an alarm if specific event occurs. The alarm can range from writing an entry in an audit log, to something significant, such as alerting 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
- Recognizing 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.

5.6 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. avoids 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.

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 and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured. IT personnel who have narrowly focused on laptops and access points commonly overlook these non- traditional networks.
- 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 from it's real MAC address.
- Man-in-the-middle attacks: A man-in-the-middle attack is an attack which is active eavesdropping. The attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker becomes capable enough to capture, insert and modify messages during message transmission.
- Accidental association: Unauthorized access to organization'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 neighboring organization's overlapping network, the user may not even know that this has occurred. However, it is a security breach in that, proprietary organization information is exposed and now there could exist a link from one organization 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. 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. WPA3 (Wi-Fi Protected Access version 3) is the latest application for encrypting Wi-Fi communication.
- Signal-hiding techniques: In order to intercept wireless transmissions, attackers first need to identify and locate wireless networks. Turning off the service set identifier (SSID) broadcast by wireless access points and reducing signal strength to the lowest level that still provides requisite coverage are the options available. 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 (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions) 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.
- 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. Default passwords should be changed 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.

5.7 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 end point (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 end-point wants to make an access to the network, the server software authenticates the device and checks whether it conforms to the security policy of the organization before allowing the access.

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

5.8 Voice-over IP Security Controls

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, and voice over broadband (VoBB). 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). In VoIP the digital information is packetized and transmitted 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, 4G or Wi-Fi.

VOIP Security

VoIP systems rely on a data network, which means security weaknesses and the types of attacks associated with any data network are possible. 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. Following are the VoIP security:

- Encryption: Encryption is a means of preserving the confidentiality of transmitted signals.
- 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.
- Anti-virus and firewalls: Computers, which use software for VoIP connections should be protected with a personal firewall, along with anti malware. This provides basic protection against attacks on the data segment that could be traversed to the voice segment.
- 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.

5.9 Vulnerability Assessment and Penetration Testing

Vulnerability Assessment and Penetration Testing (VAPT) is used by organizations 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 organization's security controls or to gain unauthorized access to its information and information systems.

Team of experts performs a VAPT. 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 organization's information system infrastructure may create exposures not anticipated during the penetration testing. Hence organizations perform these tests periodically.

Penetration Testing Scope

The scope of a penetration testing is to determine whether an organization's information security vulnerabilities can be exploited and its systems may be compromised. Penetration testing can have a number of secondary objectives, including testing the security incident identification and response capability of the organization, exploiting vulnerabilities, testing employee security awareness or testing users' compliance with information security policies.

Penetration Testing Strategies

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

External testing: External testing refers to attacks on the organization's network perimeter using procedures performed from outside the organization'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: It is performed from within the organization's information systems environment. The focus is to understand what could happen if the network perimeter were successfully penetrated or what an authorized user could do to penetrate specific information resources within the organization's network.

Targeted testing: (often referred to as the "lights-turned-on" approach) involves both the organization'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 organization'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 a complete a picture of security vulnerabilities and response capabilities of the organization.

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 organizations offer access to core business functionality through web-based applications. 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 such attack that will render it inoperable. 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 dialing: War dialing 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 organization's network. 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 organization'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 users, introduces 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 organization'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 organization's employees, suppliers and contractors, to gather information and penetrate the organization'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 organization's people to contribute to, or prevent, unauthorized access to information and information systems.

Risks Associated with Penetration Testing

While management sponsors the penetration testing activities, however, such testing represents 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 organization being vulnerable to external attacks.
- Generally, external experts perform penetration testing, hence it is necessary to enforce non- disclosure agreement and also classify content of report as confidential, since it will contain the vulnerabilities within the system.

5.10 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 needs lot of efforts and resources. There are various tools available in market that helps organizations in collecting these logs, co-relating them based on possible use cases and generate alerts for important logs. This way the efforts can be minimized. These tools are known as Security Incident and event management (SIEM) tools. Organizations use these tools and establish a security operations center (SOC) to monitor these logs, analyse alerts and record incidents and events to be responded. Also resources required to manage these tools are specially trained and skilled.

5.11 Auditing Network Security Controls

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 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
- Recognizing 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 with respect to 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 that outside the organization's control
- Evaluating logical network security policies and practices
- Evaluate network event logging and monitoring
- 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 authorization, management of components and middleware change management.

5.12 Summary

Networks are veins of market place. Organizations cannot imagine implementing information system without networks. Networks have added most important attribute to business performance, that is efficiency. However it is not without risks. This has helped organizations in expanding their business empire and also attackers, in remaining anonymous. Most security breaches today are due to availability of networks. And therefore it is most essential for organizations to protect their networks, in order to ensure that reasonable security has been implemented. IS auditors, 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

Cryptography is the science and art of coding messages, provide us a method to transmit messages over open networks, like Internet and still achieve the objectives of confidentiality, integrity, authenticity and non-repudiation. Digital certificates provide a means to digitally sign the message. PKI offers us the infrastructure to manage the Asymmetric keys, and a means of certifying the authenticity of holder of key. Cryptographic systems provide ability of secure communication over networks. Many Secure protocols and frameworks have application of cryptographic techniques like SSL, HTTPS, IPsec, SSH, SET and S-MIME to name a few.

5.13 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 organization in getting assurance on:
   A. Communication delivery
   B. Data availability
   C. Data integrity
   D. Data confidentiality
3. While auditing organization'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 center (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 does not use system resources for execution of malicious codes?
   A. Virus
   B. Logic bomb
   C. Trojan
   D. Worm

5.14 Answers and Explanations

1. A is correct answer. Other methods are active attacks on network after getting information about networks.
2. C is correct answer. Message digest is a hash function that helps in confirming integrity of data communicated over network.
3. B is correct answer. Network segmentation or zoning is first control to implement network security. Other controls depend upon segmentation.
4. B is correct answer. 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 is correct answer. 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 roles of network team.
6. C is correct answer. Intrusion detection detects the possible intrusion attempt. It does not prevent or corrects it. It is a control implemented using technology.
7. B is correct answer. It is most essential to get consent from affected asset owners 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 is correct answer. 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 is correct answer. Social engineering attack is attack on human and hence no technology can prevent it. Awareness training best prevents it.
10. D is correct answer. Worms are self-executable. Rest of the options use system resources for execution of malicious codes.

References

- Security in Computing, 3rd Edition, By Charles P. Pfleeger, Shari Lawrence Pfleeger Published Dec 2, 2002 by Prentice Hall.
- ISA 2.0 Background Study Material
- http://compnetworking.about.com/
- http://theirm.org/
- http://www.cert.org/
- http://www.isaca.org/
- http://www.iso.org/iso/home/standards/iso31000.htm
- http://www.webopedia.com
- https://na.theiia.org/Pages/IIAHome.aspx
- https://www.dataprotection.ie/
- www.ehow.com
- www.en.wikipedia.org
- www.firesafetyinstitute.org
- www.resources.infosecinstitute.com/access-control-models-and- methods
- www.technet.microsoft.com/en-us
- https://owasp.org/www-project-top-ten/
- https://en.wikipedia.org/wiki/Threat_model#Threat_modeling_tools
- https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model)
- https://en.wikipedia.org/wiki/STRIDE_(security)
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf
- https://en.wikipedia.org/wiki/Separation_of_duties

Notes

Notes