Chapter – 9

Drafting of IS Security Policy, Audit Policy, IS Audit Reporting- A Practical Perspective

Prepared By:
Jainam Shah
Email Id – shahjainam2308@yahoo.com

INTRODUCTION

- ➔ It is presumed that the information required by the Business managers is **available** all the time; it is **accurate**, it is **reliable** and **no unauthorized disclosure** of the same is made.
- ➔ Further, it is also presumed that the virtual business organization is up and running all the time on **24*7 basis** (24 hours, 7 days a week).
- ➔ However, in reality, the **technology-enabled and technology-dependent** organizations are **more vulnerable to security threats** than ever before.
- ➔ The **denial of service attacks** on the web sites of yahoo.com, amazon.com and lot of other web sites in February 2000 is a case in point. Those web sites were down for several hours to a few days jeopardizing the business of those organizations.
- ➔ The virus threat is real. The horror stories of **'Melissa' and 'I love you'** are fresh in the minds of those organizations, which were affected by them.
- ➔ Further, the hacking and cracking on the Internet is real threat to virtual organizations, which are vulnerable to information theft and manipulations.

IMPORTANCE OF INFORMATION SECURITY (9.1)

➔ Information travels through cyberspace on a routine basis, the significance of information is widely accepted.

➔ Organizations depend on

- ✡ Timely
- ✡ Accurate
- ✡ Complete
- ✡ Valid
- ✡ Consistent
- ✡ Relevant
- ✡ Reliable

Information.

➔ There are not only many direct and indirect benefits from the use of information systems, there are also many direct and indirect risks relating to the information systems.

➔ These risks have led to a gap between the need to protect systems and the degree of protection applied. **This gap is caused by:**

- ☆ Widespread use of technology.
- ☆ Interconnectivity of systems.
- ☆ Elimination of distance, time, and space as constraints.
- ☆ Unevenness of technological changes.
- ☆ Devolution of management and control.
- ☆ Attractiveness of conducting unconventional electronic attacks against organizations.

- ☆ External factors such as legislative, legal, and regulatory requirements or technological developments.

➔ Security failures may result in both **financial losses and intangible losses** such as unauthorized disclosure of competitive or sensitive information.

Threats May Be

Intentional or Unintentional

Internal or External

➔ Adequate measures for information security help to ensure the smooth functioning of information systems and protect the organization from loss caused by security failures.

INFORMATION SYSTEM SECURITY (9.2)

- Relates to the protection of valuable assets against loss, disclosure, or damage.
- Securing valuable assets from threats, sabotage, or natural disaster with **Physical safeguards** such as
  - locks
  - perimeter fences
  - insurance

  is commonly understood and implemented by most organizations.
- However, security must be expanded to include **Logical and other technical safeguards** such as
  - user identifiers
  - passwords
  - firewalls

  which are not understood.
- This concept of security applies to all information.
- The protection is achieved through a layered series of **Technological and non-technological safeguards** such as

  Physical security measures
  - user identifiers
  - passwords
  - smart cards
  - biometrics

- firewalls

➔ **Security Objective:**

"The **protection of the interests** of those

- Who relying on information,
- the information systems,
- communications that deliver the information

from harm resulting from failures of **(ICA)**

- Integrity
- Confidentiality
- Availability".

Confidentiality: Prevention of the unauthorized **disclosure** of information.

Integrity: Prevention of the unauthorized **modification** of information.

Availability: Prevention of the unauthorized **withholding** of information.

WHAT INFORMATION IS SENSITIVE? (9.2.1)

➔ **Strategic Plans** – Strategic Plans are crucial to the company's success. E.g.- Coke & Pepsi.

➔ **Business Operations** – This is the case when one company can provide service profitability at a lower rate than the competition. Carelessness often results in its compromise.

➔ **Finances** – Salaries and wages related charges normally comprise the majority of fixed cost. Lower Cost in this direct increase the contribution.

ESTABLISHING BETTER INFORMATION PROTECTION (9.2.2)

What steps do they need to take to keep all of their critical information protected?

- ➔ **Not all data has the same value** – Book v/s Jewellery
- ➔ **Know where the critical data resides**
- ➔ **Develop an access control methodology** – Access control extends from hosts to Network
- ➔ **Protect information stored on media**
- ➔ **Review hardcopy output** – Employee's diary work should be reviewed.

PROTECTING COMPUTER HELD INFORMATION SYSTEM (9.3)

We need to define a few basic ground rules that must be addressed sequentially:

Rule 1:

We need to know that **'what the information systems are'** and **'where these are located'**.

Rule 2:

We need know the **value of the information** held and how difficult it would be to recreate if it were damaged or lost.

Rule 3:

We need to know that **'who is authorized to access the information'** and **'what they are permitted to do with the information'**.

Rule 4:

We need to know that '**how quickly information needs to be made available** should and it become unavailable for whatever reason (loss, unauthorized modification, etc.) '

- ➔ There are **two basic types of protection** that an organization can use: Preventative and Restorative.

PREVENTATIVE INFORMATION PROTECTION (9.3.1)

- **Physical:** Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems.
- **Logical (Technical):** Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems.
- **Administrative:** Security Awareness, User Account Revocation, Policy.

RESTORATIVE INFORMATION PROTECTION (9.3.2)

- If an organization **cannot recover or recreate critical information** systems in an acceptable time period, the organization will suffer and possibly have to **go out of business.**
- Information system backup does not simply involve backing up "just the valuable information," but it frequently also means backing up the system as well.
- Here are a **few questions** that any restorative information system protection program must address:
  - Has the recovery process been tested recently?
  - How long did it take?
  - How much productivity was lost?
  - Did everything go according to plan?
  - How much extra time was needed to input the data changes since the last backup?

INFORMATION SECURITY POLICY (9.4)

- ➔ A Policy is a **plan or course of action**, designed to influence and determine decisions, actions and other matters.
- ➔ The security policy is a **set of laws, rules, and practices** that regulates how assets, including sensitive information are managed, protected, and distributed within the user organization.

ISSUES TO ADDRESS: (9.4.1)

- ☆ a definition of information security,
- ☆ why information security is important to the organization, and its goals and principles,
- ☆ a brief explanation of the security policies, principles, standards and compliance requirements,
- ☆ definition of all relevant information security responsibilities
- ☆ Reference to supporting documentation.

- ➔ Auditor should ensure that policy is readily available; employees are aware of its existence and understand its contents.
- ➔ Training and awareness issue is must.

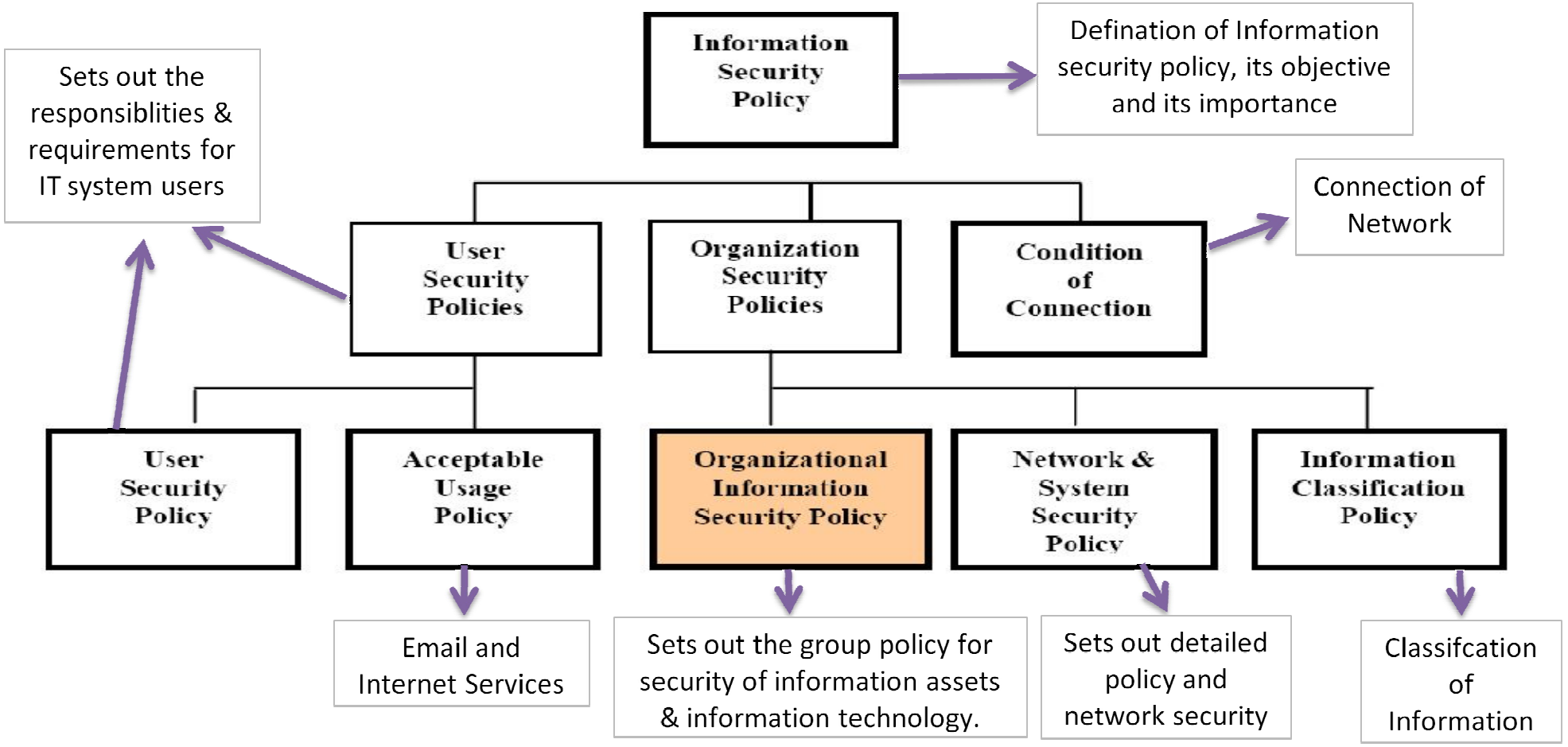
MEMBERS OF SECURITY POLICY (9.4.2)

Management members: who have budget and policy authority.

Technical group: who know what can and cannot be supported.

Legal experts: who know the legal ramifications of various policy charges.

Types of Information Security & Their Hierarchy (9.5)



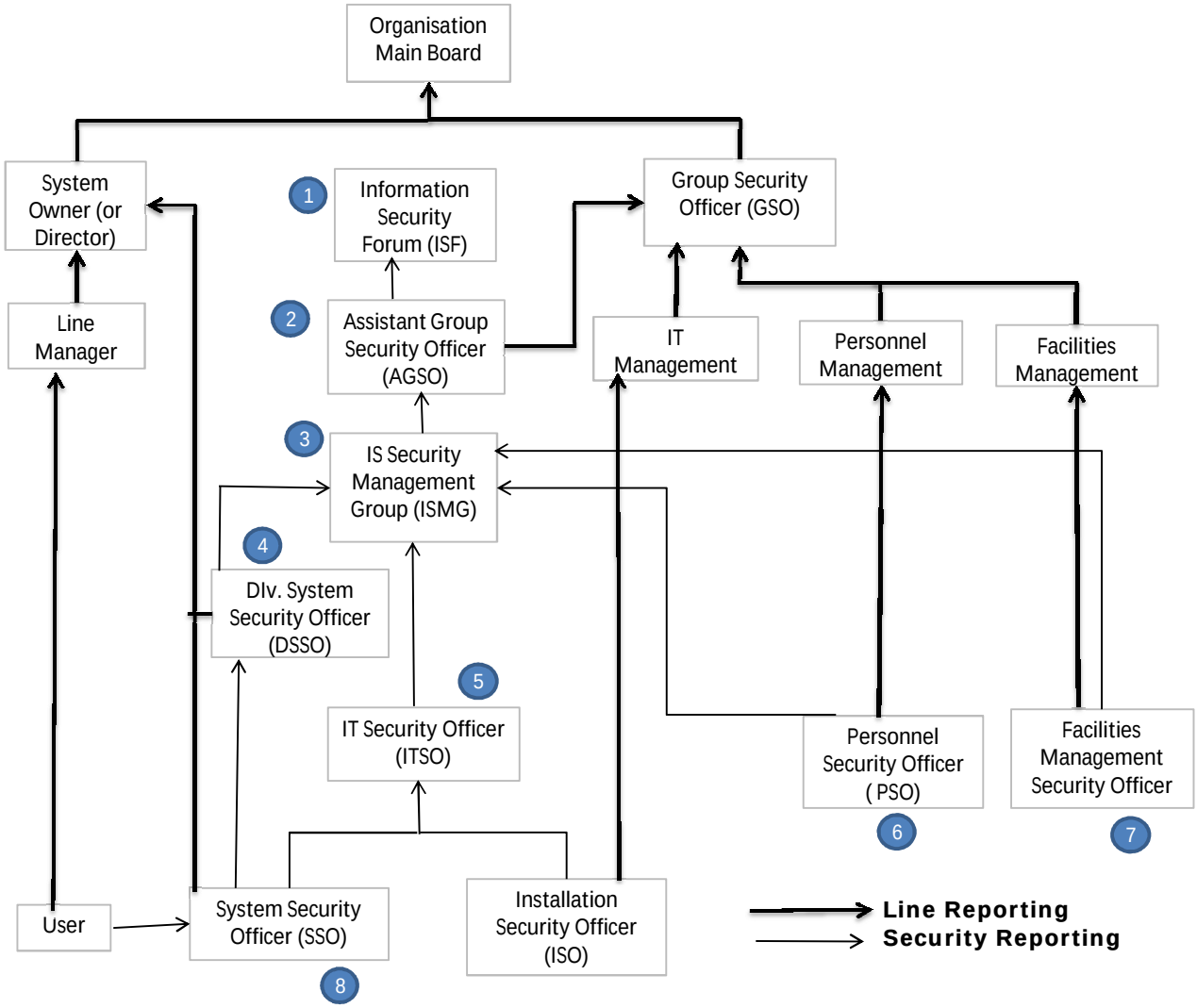
COMPONENTS OF THE SECURITY POLICY (9.5.1)

- Purpose and Scope of the Document and the intended audience
- Underlying Technical Policy
- ☆ **IT** Operations management
- ☆ **IT** Communications
- ➔ The **Security** Infrastructure
- ➔ **Security** policy document maintenance and compliance requirements
- ➔ **Security** organization Structure
- ➔ Physical and Environmental **Security**
- ✓ Inventory and **C**lassification of assets
- ✓ **D**escription of technologies and computing structure
- ✡ System Development and Maintenance Controls
- ✡ Business Continuity Planning
- ✡ Legal Compliances

PURPOSE AND SCOPE (9.5.2)

- ➔ Deny authorized access to any IT resources, and Restrict access to data.
- ➔ The security controls will allow the required services to be available to authorized users only.
- ➔ **Scope**
    - ✡ How far the policy would be applicable
    - ✡ to whom it would be applicable
    - ✡ the period for which the policy would be applicable.

Security Organisation Structure (9.5.3)



RESPONSIBILITY ALLOCATION (9.5.4)

- ➔ An **owner** would be appointed for each information asset.
- ➔ All **staff** should be aware of the need for Information Security and their responsibilities.
- ➔ All the tasks have been completed successfully and the System **Owner** is satisfied.
- ☆ All **new network** communications links must be approved.
- ☆ A **contact list** of organizations that may be required in the event of a security incident to be maintained.
- ✡ Risk assessments for all **third party access** to the information assets must be carried out.
- ✡ Access by **third parties** to all material related to the IT Network and infrastructure must be strictly limited and controlled.
- ✡ There should be a Conditions of Connection agreement in place for all **third party** connections.

ASSET CLASSIFICATION AND SECURITY CLASSIFICATION (9.5.5)

- ➔ An inventory of assets must be maintained. This must include physical, software and information assets.
- ➔ A formal, documented classification scheme should be in place and all staff must comply with it.
- ➔ Owner of an item of information should provide a security classification, where appropriate.

- ➔ The handling of information, which is protectively marked CONFIDENTIAL or above must be specifically approved.
- ➔ Exchanges of data and software between organizations must be controlled.
- ➔ Organizations to whom information is to be sent must be informed of the protective marking associated with that information, in order to establish that it will be handled by personnel with a suitable clearance corresponding to the protective marking.
- ➔ Procedures for information labeling and handling must be agreed and put into practice.
- ➔ Waste must be disposed of appropriately and securely.

ACCESS CONTROL (9.5.6)

- ➔ Access controls must be in place to prevent unauthorized access.
- ➔ Requirement for access must be reviewed regularly.
- ➔ System Owners are responsible for approving access to systems and they must maintain log of the system.
- ☆ **Users** should be granted access to systems only up to the level required.
- ☆ The registration and de-registration of **users** must be formally managed.
- ☆ Access rights must be deleted for **individuals** who leave or change jobs.
- ☆ Unique User Identifier (**User-id**)
- ☆ Not to permit to use another person's **user-id**.
- ✓ **PCs and terminals** should never be left unattended whilst they are connected to applications or the network.

- ✓ **Passwords Policy** should be defined:
  - ❖ structure of passwords
  - ❖ duration of the passwords
  - ❖ Passwords must be kept confidential
- ✓ **Mobile computing** - When using mobile computing facilities, such as laptops, notebooks, etc., special care should be taken to ensure that business information is not compromised, particularly when the equipment is used in public places.

INCIDENT HANDLING (9.5.7)

- ➔ Specific procedures must be introduced to identify weaknesses or trends.
- ➔ All staff must be made aware of the process.
- ➔ Adequate records must be maintained and inspected.

PHYSICAL AND ENVIRONMENTAL SECURITY (9.5.8)

- ➔ Physical security should be maintained and checks must be performed to identify all vulnerable areas within each site.
- ➔ The IT infrastructure must be physically protected.
- ➔ Access to secure areas must remain limited to authorized staff only.
- ➔ Confidential and sensitive information and valuable assets must always be securely locked away when not in use.
- ➔ PCs and terminals should never be left unattended whilst they are connected to applications or the network.
- ➔ Supplies and equipment must be delivered and loaded in an isolated area to prevent any unauthorized access to key facilities
- ➔ Equipment, information or software must not be taken off-site without proper authorization.

AUDIT POLICY (9.6)

PURPOSE OF THE AUDIT POLICY (9.6.1)

➔ The Audit is done to protect entire system from the most common security threats which includes the following:

- ❖ Access to confidential data.
- ❖ Unauthorized access.
- ❖ Password disclosure compromise.
- ❖ Virus infections.
- ❖ Denial of service attacks.
- ❖ Open ports.
- ❖ Unrestricted modems unnecessarily open ports.

➔ Objective of the audit policy

- ❖ Safeguard the Information System Assets.
- ❖ Maintain the Data Integrity.
- ❖ Maintain the System Effectiveness.
- ❖ Ensure System Efficiency.
- ❖ Comply with Information System related policies, guidelines, instructions.

SCOPE OF THE AUDIT POLICY (9.6.2) (FATPD)

- ➔ **F**acilities
- ➔ **A**pplication systems
- ➔ **T**echnology
- ➔ **P**eople
- ➔ **D**ata

WHAT AUDIT POLICY SHOULD DO? (9.6.3)

- ➔ The Audit Policy should lay down the responsibility of audit.
- ➔ The audit may be conducted by internal auditors or external auditors. Information
- ➔ System Auditors should be independent of the activities they audit.
- ➔ Independence permits the auditors to render impartial and unbiased judgment.
  - ☆ The Policy should lay out the **periodicity of reporting** and the **authority to whom the reporting** is to be made
  - ☆ Minimum qualification and experience requirements of the auditors.
  - ☆ All information system auditors will sign a **declaration of fidelity** and **secrecy** before commencing the audit work.
  - ☆ Extent of testing to be done under the various phases of the audit
    - ✡ Planning
    - ✡ Compliance Testing
    - ✡ Substantive Testing

DOCUMENTED AUDIT PROGRAM

- ➔ Collecting, analyzing, interpreting, and documenting information during the audit.
- ➔ Objectives of the audit.
- ➔ Scope, nature, and degree of testing
- ➔ Identification of technical aspects, risks, processes, and transactions which should be examined.
- ➔ Procedures for audit will be prepared prior to the commencement of audit work.

ACCESS RIGHTS GIVEN TO AUDITORS (WI²RLO)

- ➔ Access to **w**ork areas. (labs, offices, cubicles, storage areas)
- ➔ Access to **i**nformation
- ➔ Access to **i**nteractively monitor and log traffic on networks.
- ➔ Access to **r**eports / documents created during internal audit.
- ➔ User **l**evel and/or system **l**evel access to any computing or communications device

COMPLIANCE TESTING AREAS (BAPASSO)

- ➔ **B**usiness Continuity Controls.
- ➔ **A**ccess Controls.
- ➔ **P**hysical and Environmental Controls.
- ➔ **A**pplication Controls.
- ➔ **S**ystem development and Documentation Controls.
- ➔ **S**ecurity Management Controls.
- ➔ **O**rganizational and Operational Controls.

AUDIT WORKING PAPERS & DOCUMENTATION (9.7)

Working papers should record

- ❖ the audit plan,
- ❖ the nature,
- ❖ timing,
- ❖ extent of auditing procedures performed,
- ❖ the conclusions drawn from the evidence obtained.

➔ The form and content of the **working papers are affected** by matters such as:

- ❖ The nature of the engagement,
- ❖ The form of the auditor's report,
- ❖ The nature and complexity of client's business, and
- ❖ The nature and condition of client's records and degree of reliance on internal controls.

Permanent audit file normally includes:

- ➔ The organization structure of the entity.
- ➔ The IS policies of the organization.
- ➔ The historical background of the information system in the organization.
- ➔ Copies of important legal documents relevant to audit.
- ➔ Study and evaluation of the internal controls.
- ➔ Audit reports and observations of earlier years.
- ➔ Management letters issued by the auditor.

Current file normally includes:

- ➔ Acceptance of appointment letter.
- ➔ Planning process of the audit and audit programme.
- ➔ Nature, timing, and extent of auditing procedures performed and the results of such procedures.
- ➔ Letters and notes concerning audit matters, including material weaknesses in relevant internal controls communicated or discussed with the client.
- ➔ Letters of representation and confirmation received from the client.
- ➔ Conclusions reached by the auditor including the exceptions and unusual matters.
- ➔ Copies on the data and system being reported on and the related audit reports.

IS AUDIT REPORT (9.8) (TCS/I/FOA)

- IS audit report is an end product of information system audit, conducted by an IS auditor.
- This report is communicated to management with opinions.
- Though there is no standard format or guidelines for preparation of this report, but overall this report may have the following:
  - **T**itle & cover page.
  - **C**ontent table
  - **S**ummary (Table)
  - **I**ntroduction:
    - Background of IT environment or context
    - Purpose of audit
    - Scope of audit
    - Methodology used for auditing
  - **F**indings
  - **O**pinion
  - **A**ppendices