CHAPTER 9

DRAFTING OF IS SECURITY POLICY, AUDIT POLICY, IS AUDITING REPORTING- A PRACTICAL PERSPECTIVE

⇨ IMPORTANTANCE OF INFORMATION SYSTEM SECURITY

- ☞ Beside 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** over more conventional physical attacks against organizations; and
  - ✳ **EXTERNAL FACTORS** such as legislative, legal, and regulatory requirements or technological developments.
- ☞ Security failures may result in both **FINANCIAL LOSSES AND/OR INTANGIBLE LOSSES** such as unauthorized disclosure of competitive or sensitive information.
- ☞ Threats to information systems may arise from **INTENTIONAL OR UNINTENTIONAL ACTS** and may come from **INTERNAL OR EXTERNAL SOURCES**. The threats may originated from, among others:
  - ✳ Technical conditions (program bugs, disk crashes),
  - ✳ natural disasters (fires, floods),
  - ✳ environmental conditions (electrical surges),
  - ✳ human factors (lack of training, errors, and omissions),
  - ✳ unauthorized access (hacking),
  - ✳ viruses,
  - ✳ Other threats, such as business dependencies (reliance on third party communications carriers, outsourced operations, etc.)

⇨ INFORMATION SYSTEM SECURITY

- ☞ Security means **PROTECTION** & Information Security means **PROTECTION OF INFORMATION**.

- Security relates to the **PROTECTION OF VALUABLE ASSETS** against loss, disclosure, or damage.
- **PHYSICAL SAFEGUARDS** for securing valuable assets from threats, sabotage, or natural disaster. For e.g. locks, perimeter fences, and insurance is commonly.
- Security must be expanded to include **LOGICAL AND OTHER TECHNICAL SAFEGUARDS** such as user identifiers, passwords, firewalls, etc. This concept of security applies to all information.
- In this context, the "**VALUABLE ASSETS** are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium".
- The data or information is protected against harm from threats that will lead to its loss, inaccessibility, alteration, or wrongful disclosure.
- The protection is achieved through a layered **SERIES OF TECHNOLOGICAL AND NON-TECHNOLOGICAL SAFEGUARDS.**

⇨ SECURITY OBJECTIVE (CIA)

- The objective of information system security is
  - "The protection of the interests of those relying on information, and
  - the information systems and communications
  - That delivers the information, from harm resulting from failures of confidentiality, integrity, and availability".
- For any organization, the security objective comprises three universally accepted attributes:
  - **C**ONFIDENTIALITY: Prevention of the **UNAUTHORIZED DISCLOSURE** of information.
  - **I**NTEGRITY: Prevention of the **UNAUTHORIZED MODIFICATION** of information.
  - **A**VAILABILITY: Prevention of the **UNAUTHORIZED WITHHOLDING** of information.
- The relative priority and significance of confidentiality, integrity and availability vary according to the data within the information system and the business context in which it is used.

⇨ WHAT INFORMATION IS SENSITIVE (FBS: Fake Balance Sheet)

Following types of information is normally considered sensitive information.

- **F**inancial Information:
  - Financial information such as salaries, wages customer orders position, cash & bank positions etc are very crucial and should not be made public or disclosed.
  - When a competitor knows specific information about a company's wages, he may be able to price its product accordingly.
  - As such, the damage to the organization may be significant.
- **B**usiness operation information:
  - It consists of an organization **PROCESS AND PROCEDURES** which are related to production & technologies which are proprietary in nature.
  - And it is necessary to secure this type of information.

- ✳ While most of the organization prohibits the sharing of data, any type of carelessness may result in inadvertent (negligent) storage of data on authorized systems, unprotected laptops and failure of secure magnetic media.

☞ **S**trategic Plans:

- ✳ Strategic plans are very **CRUCIAL FOR SUCCESS** of organization and it is required that these strategic plans should be **WELL PROTECTED**.
- ✳ These plans normally involves the decision making part of the management.
- ✳ For instance a company discovers new areas of launching its product, but due to weak information security system the same is being exploited by its competitors. This may result in loss to the former company.

⇨ ESTABLISHING BETTER INFORMATION PROTECTION

Businesses hold such a lot of data. Following points may be considered in determining steps need to take to keep all of their critical information protected:

☞ **Not all data has the same value**.

- ✳ Organizations must determine the value of the different types of information.
- ✳ It helps plan for the appropriate levels of protection.
- ✳ As such the information may be handled and protected differently.

☞ **Know where the critical data resides**.

- ✳ A different type of information requires different levels of protection, hence identifying where each is located enables an organization to establish an integrated security solution.
- ✳ This approach also provides significant cost benefits, as the company does not need to spend more on protecting data than the data itself is worth.
- ✳ Protection solutions must be based on the most valuable information assets.

☞ **Develop an access control methodology.**

- ✳ Protect access in needed to safeguard cause damage, unintended disclosure and wrongful coping the data.
- ✳ For important data, this access control (and the associated auditing) should extend to the file level.
- ✳ Such access control extends from the host to the network

☞ **Protect information stored on media.**

- ✳ companies should control magnetic media to reduce the loss of software (both application and operating system).
- ✳ It should be careful, when migrating from one platform to another.

☞ **Review hardcopy output.**

- ✳ The hardcopy output of employees' daily work should also be reviewed.
- ✳ Although strategic plans in their final forms may be adequately protected, what measures are used to safeguard all drafts and working papers? What information is regularly placed in the recycle or trash containers without thought to its value?

⇨ PROTECTING COMPUTER-HELD INFORMATION SYSTEMS

Prior to know the details of **`HOW TO PROTECT THE INFORMATION SYSTEMS'**, we need to define a **FEW BASIC GROUND RULES** that must be **ADDRESSED SEQUENTIALLY**. These rules are:

☞ 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.)

⇨ PREVENTATIVE INFORMATION PROTECTION

Explain the basic types of Information Protection that an Organization can use. (N'09- 5 Marks)

The two basic types of information protection that an organization can use are given as follows:

1. Preventative Information Protection, and
2. Restorative Information Protection.

1. Preventative Information Protection:
   It is based on **USE OF SECURITY CONTROLS**, which itself is a group of three types of controls:
   - ✳ **PHYSICAL CONTROLS** deal with Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems,
   - ✳ **LOGICAL CONTROLS** deal with Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems, and
   - ✳ **ADMINISTRATIVE CONTROLS** deal with Security Awareness, User Account Revocation, and Policy.

2. Restorative Information Protection:
   - ✳ 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.
   - ✳ Planning & operating an effective & timely information **SYSTEM BACKUP AND RECOVERY PROGRAM IS VITAL**.
   - ✳ The restorative information protection program must address the following:
     - 🖋 Whether the recovery process has been evaluated and tested recently?
     - 🖋 The time taken for restoration,
     - 🖋 The quantum of productivity loss,
     - 🖋 The strict adherence of plan, and
     - 🖋 The time needed to input the data changes since the last backup.

Other than organization can use

3. Holistic Protection:
   - ✳ Protection must be done holistically and give the organization the appropriate level of security.

- One must be prepared for the unexpected & unknown and worst event to happen and immediately recover from these events, if they occur.

⇨ INFORMATION SECURITY POLICY

The Information Security Policy of an organization has been defined and documented as given below:
"Our organization is committed to ensure Information Security through established goals and principles. Responsibilities for implementing every aspect of specific applicable proprietary and general principles, standards and compliance requirements have been defined. This is reviewed at least once a year for continued suitability with regard to cost and technological changes." (M'09- 5 Marks)

- 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.**
- An INFORMATION SECURITY POLICY addresses many issues such as
  - disclosure, integrity and availability concerns,
  - who may access what information and in what manner,
  - basis on which access decision is made,
  - Maximized sharing versus least privilege,
  - Separation of duties,
  - who controls and who owns the information, and
  - Authority issues.
- Issues to address: This policy does not need to be **EXTREMELY EXTENSIVE**, but clearly state senior **MANAGEMENT'S COMMITMENT** to information security, be under change and version **CONTROL** and be **SIGNED** by the appropriate senior manager. The policy should at least address the following issues:
  - a **DEFINITION** of information security,
  - reasons 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, and
  - reference to supporting **DOCUMENTATION**
- Auditors Role:

- ✳ The auditor should ensure that the policy is **READILY ACCESSIBLE** to all employees and that all employees are **AWARE OF ITS EXISTENCE AND UNDERSTAND ITS CONTENTS**.
- ✳ The auditors should **REVIEW ANY DECLARATIONS** to the contrary with care.
- ✳ The auditor should also ensure that the policy has an **OWNER WHO IS RESPONSIBLE** for its maintenance and that it is **UPDATED** responding to any changes affecting the basis of the original risk assessment.

☞ In the stated scenario of the question, the ISMS Policy of the given organization does not address the following issues:

- ✳ Definition of information security,
- ✳ Reasons why information security is important to the organization,
- ✳ A brief explanation of the security policies, principles, standards and compliance, and
- ✳ Reference to supporting documents

Note: This Points exclusive for this case study only. This it last point of this question.

☞ Member of Security Policy (MTL):

❖ Security has to encompass managerial, technological and legal aspects. Security policy broadly comprises the following three groups of management:

- ✳ **M**ANAGEMENT members who have budget and policy authority,
- ✳ **T**ECHNICAL group who know what can and cannot be supported, and
- ✳ **L**EGAL experts who know the legal ramifications of various policy charges.

❖ Conclusion:

- ✳ Information security policies must always take into account **BUSINESS REQUIREMENTS** i.e. the principles and objectives adopted by an organization to support its operations and information processing.
- ✳ E-commerce security is an example of such business requirements.
- ✳ Furthermore, policies must consistently take into account **THE LEGAL, STATUTORY, REGULATORY AND CONTRACTUAL REQUIREMENTS** that the organization and its professional partners, suppliers and service providers must respect.

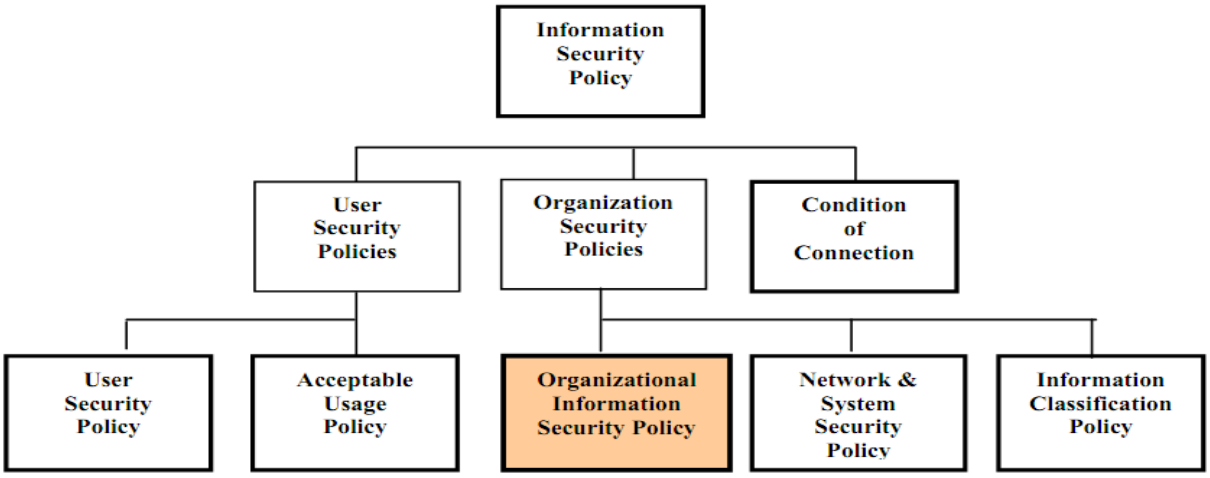
⇨ TYPES OF INFORMATION SECURITY POLICY AND THEIR HIERARCHY

Various types of information security policies are:

1. Information Security Policy: This policy provides
   - ✳ a definition of Information Security,
   - ✳ its overall objective and
   - ✳ The importance that applies to all users.
2. User Security Policy:
   - ✳ This policy sets out the **RESPONSIBILITIES AND REQUIREMENTS** for all IT system users.
   - ✳ It provides security terms of reference for Users, Line Managers and System Owners.
3. Acceptable Usage Policy: This sets out the policy for **ACCEPTABLE USE** of email and Internet services.
4. Organizational Information Security Policy:

- ✳ This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information.
- ✳ Though it is positioned at the bottom of the hierarchy, it is **THE MAIN IT SECURITY POLICY** document.

5. Network & System Security Policy: This policy sets out
   - ✳ detailed policy for system and network security and
   - ✳ applies to IT department users
6. Information Classification Policy: This policy sets out the policy for the classification of information.
7. Conditions of Connection:
   - ✳ This policy sets out the Group policy for **CONNECTING TO THEIR NETWORK**.
   - ✳ It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.



⇨ COMPONENTS OF THE SECURITY POLICY: A good security policy should clearly state the following:

- ☞ **PURPOSE AND SCOPE** of the document and the intended **AUDIENCE**.
- ☞ The security **INFRASTRUCTURE**.
- ☞ Security policy document **MAINTENANCE AND COMPLIANCE** requirements.
- ☞ **INCIDENT** response mechanism and incident reporting.
- ☞ Security organization **STRUCTURE**.
- ☞ Inventory and classification of **ASSETS**.
- ☞ Description of **TECHNOLOGIES AND COMPUTING STRUCTURE**.
- ☞ **PHYSICAL AND ENVIRONMENTAL** security.
- ☞ Identify management and **ACCESS CONTROL**.
- ☞ IT **OPERATIONS** management.
- ☞ IT **COMMUNICATIONS**.
- ☞ **SYSTEM DEVELOPMENT AND MAINTENANCE** controls.
- ☞ Business continuity planning.
- ☞ Legal compliances.
- ☞ **MONITORING AND AUDITING** Requirements.
- ☞ Underlying **TECHNICAL POLICY**.

⇨ RESPONSIBILITY ALLOCATION

The responsibilities for the management of Information Security should be set out in this policy.

- ☞ An owner would be appointed for each information asset
- ☞ All staff should be aware of the need for Information Security and should be aware of their responsibilities.
- ☞ 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 and the IT Network 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.
- ☞ All outsourcing contracts must detail All major changes to software and hardware including major updates and new versions must be approved. It is not permissible to make the changes to a live system until tests have security responsibilities

⇨ ASSET AND SECURITY CLASSIFICATION

- ☞ An inventory of assets must be maintained. This must include physical, software and information assets.
- ☞ A formal, documented classification scheme (as set out in the Information Classification Policy) should be in place and all staff must comply with it.
- ☞ The originator or 'owner' of an item of information (e.g. A document, file, diskette, printed report, screen display, e-mail, etc) should provide a security classification, where appropriate.
- ☞ The handling of information, which is protectively marked CONFIDENTIAL or above must be specifically approved (i.e. above RESTRICTED).
- ☞ Exchanges of data and software between organizations must be controlled.
- ☞ Appropriate procedures for information labeling and handling must be agreed and put into practice.
- ☞ Classified waste must be disposed of appropriately and securely

⇨ ACCESS CONTROL

- ☞ Access controls must be in place to prevent unauthorized access to information systems and computer applications
- ☞ Access must only be granted in response to a business requirement. Formal processes must be in place to provide individuals with access. The requirement for access must be reviewed regularly.
- ☞ System Owners are responsible for approving access to systems and they must maintain records of who has access to a particular system and at what level. The actual access controls in place must be audited against this record on a regular basis.
- ☞ Users should be granted access to systems only up to the level required to perform their normal business functions.
- ☞ The registration and de-registration of users must be formally managed.
- ☞ Access rights must be deleted for individuals who leave or change jobs.
- ☞ Each individual user of an information system or computer application will be provided with a unique user identifier (user id)

- ☞ It should not be permitted for an individual to use another person's user id or to log-on, to allow another individual to gain access to an information system or computer application.
- ☞ PCs and terminals should never be left unattended whilst they are connected to applications or the network. Someone may use the equipment to access confidential information or make unauthorized changes.
- ☞ Passwords Policy should be defined and the structure of passwords and the duration of the passwords should be specified. Passwords must be kept confidential and never disclosed to others.
- ☞ 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

- ☞ Security incident reporting times and approach must be consistent at all times. Specific procedures must be introduced to ensure that incidents are recorded and any recurrence is analyzed to identify weaknesses or trends.
- ☞ Procedures for the collection of evidence relating to security incidents should be standardized. All staff must be made aware of the process. Adequate records must be maintained and inspections facilitated to enable the investigation of security breaches or concerted attempts by third parties to identify security weaknesses

⇨ PHYSICAL AND ENVIRONMENTAL SECURITY:

- ☞ 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 asserts must always be securely locked away when not in use.
- ☞ Computers must never be left unattended whilst displaying confidential or sensitive information or whilst logged on to systems.
- ☞ Supplies and equipment must be delivered and loaded in an isolated area to prevent any unauthorized access to key facilities.
- ☞ Wherever practical, premises housing computer equipment and data should be located away from and protected against threats of deliberate or accidental damage such as fire and natural disaster.
- ☞ The location of the equipment room (s) must not be obvious. It should practically be located away and protected against threats of unauthorized access and deliberate or accidental damage, such as system infiltration and environmental failures.

⇨ AUDIT POLICY

What purpose the information system audit policy will serve? Briefly describe the scope of information system audit. (M'09- 10 Marks)

- ☞ PURPOSE OF THE AUDIT POLICY:
  - ✳ Purpose of the audit policy is to provide the **GUIDELINES** to the audit team to conduct

an **AUDIT OF IT BASED INFRASTRUCTURE SYSTEM**.

- ✳ The Audit is done to protect entire system from the most common security threats which includes the following:
  - Access to **CONFIDENTIAL** data
  - **UNAUTHORIZED** access of the department computers
  - **PASSWORD** disclosure compromise
  - **VIRUS** infections
  - Denial of service **(DOS)** attacks
  - Open ports, which may be accessed by outsiders
  - Unrestricted modems, unnecessarily open ports
- ✳ Audits may be conducted to ensure integrity, confidentially and availability of information and resources. The IS Audit Policy should lay out the objective and the scope of the Policy.
- ✳ An IS audit is conducted to:
  - **SAFEGUARDING** of Information System Assets/Resources
  - Maintenances of **DATA INTEGRITY**
  - Maintenance of **SYSTEM EFFECTIVENESS**
  - Ensuring **SYSTEM EFFICIENCY**
  - **COMPLIANCE** with Information System related policies, guidelines, circulars, and any other instructions requiring compliance in whatever name called.

☞ SCOPE OF IS AUDIT:

- ✳ The scope of information system auditing should encompass
  - the **EXAMINATION AND EVALUATION** of
  - the **ADEQUACY AND EFFECTIVENESS** of
  - the system of **INTERNAL CONTROL** and
  - the **QUALITY OF PERFORMANCE** by the information system.
- ✳ Information System Audit will examine and evaluate the planning, organizing, and directing processes to determine whether **REASONABLE ASSURANCE EXISTS** that objectives and goals will be achieved.
- ✳ It helps appraise the overall system of internal control.
- ✳ The scope of the audit will also include the internal control system (s) for the use and protection of information and the information system, as under:
  - Data
  - Application systems
  - Technology
  - Facilities
  - People
- ✳ The information System auditor will consider whether the information obtained from the above reviews indicates coverage of the appropriate areas.
- ✳ The information system auditor will examine, among other, the following:
  - Information system **MISSION STATEMENT** and agreed goals and objectives for information system activities.
  - **ASSESSMENT OF THE RISKS ASSOCIATED** with the use of the information systems and **APPROACH TO MANAGING THOSE RISKS**.
  - Information system **STRATEGY PLANS** to implement the strategy and

MONITORING of progress against those plans.

- Information system **BUDGET AND MONITORING OF VARIANCES**.
- **HIGH LEVEL POLICES** for information system use and the protection and monitoring of **COMPLIANCE** with these polices.
- Major **CONTRACT APPROVAL AND MONITORING** of performance of the supplier.
- Monitoring of performance against **SERVICE LEVEL AGREEMENTS**
- **ACQUISITION** of major systems and decisions on implementation.
- Impact of **EXTERNAL INFLUENCES** on information system such as internet, merger of suppliers or liquidation etc.
- **CONTROL OF REPORTS**: self-assessment reports, internal and external audit reports, quality assurance reports or other reports on Information System.
- **BUSINESS CONTINUITY PLANNING**, Testing thereof and Test results.
- **COMPLIANCE WITH LEGAL** and regulatory requirements
- Appointment, performance monitoring and **SUCCESSION PLANNING** for senior information system staff including internal information system audit management and business process owners.

☞ WHAT AUDIT POLICY SHOULD DO? :

- ✳ **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 essential to the proper conduct of audits.
- ✳ It is achieved through organizational status and objectivity.

1. The Policy should lay out the **PERIODICITY OF REPORTING AND THE AUTHORITY REPORTING**
2. A **STATEMENT OF PROFESSIONAL PROFICIENCY** may be included to sate the **MINIMUM QUALIFICATION AND EXPERIENCE** requirements of the auditors.
3. All information system auditors will **SIGN A DECLARATION** of fidelity and secrecy before commencing the audit work.
4. The policy may lay out the **EXTENT OF TESTING** to be done under the various phases of the audit
   - Planning
   - Compliance Testing
   - Substantive Testing
5. A **DOCUMENTED AUDIT PROGRAM** would be developed including the following (N' 10- 4 Marks):
   - Documentation of the information system **AUDITOR'S PROCEDURES** for collecting, analyzing, interpreting, and documenting information during the audit.
   - **OBJECTIVES** of the audit.
   - **SCOPE, NATURE, AND DEGREE OF TESTING** required achieving the audit objectives in each phase of the audit.
   - **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 and modified, as appropriate, during the course of the audit.

6. The policy should determine when and to whom the **AUDIT RESULTS WOULD BE REPORTED AND COMMUNICATED**. It would define the access rights to be given to the auditors. This access may include:
   - User level and/or system level access to any computing or communications
   - Device
   - Access to information (electronic, hardcopy, etc.) that may be produced,
   - transmitted or stored on respective Dept. equipment or premises
   - Access to work areas (labs, offices, cubicles, storage areas, etc.)
   - Access to reports / documents created during internal audit.
   - Access to interactively monitor and log traffic on networks.
7. The Policy should outline the **COMPLIANCE TESTING AREAS** e.g.
   - Organizational and Operational Controls
   - Security Management Controls
   - System development and Documentation Controls
   - Application Controls
   - Physical and Environmental Controls
   - Access Controls
   - Business Continuity Controls, etc.
8. The auditor will carry out **SUBSTANTIVE TESTING** wherever the auditor observes weakness in internal control or where risk exposure is high. The auditor may also carry out such tests to gather additional information necessary to form an audit opinion.
9. The Audit Policy would define the **COMPULSORY AUDIT WORKING PAPERS** to be maintained and their formats.

⇨ DOCUMENTATION IN AN IS AUDIT

You have been asked to conduct an I.S. Audit for a bank. 1. How will you develop a documented audit program? (Refer point 5 of what audit policies do?) 2. What kind of working papers and documentation you will prepare? (N'09- 10 Marks)

☞ Audit Working Papers and Documentation:

- ✳ Working papers should
  - Record the audit plan,
  - the nature, timing and extent of auditing procedures performed, and
  - The conclusions drawn from the evidence obtained.
- ✳ All significant matters which require the exercise of judgment, together with the auditor's conclusion thereon, should be included in the working papers.
- ✳ 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**
  - The nature and condition of **CLIENT'S RECORDS** and degree of reliance on **INTERNAL CONTROLS**.

- working paper files may be classified as
  - Permanent Audit Files
  - Current Audit Files

  - Permanent Audit Files: Permanent Audit Files which are updated currently with **INFORMATION OF CONTINUING IMPORTANCE** to succeeding audits. The 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.
    - Extracts of copies of important legal documents relevant to audit.
    - A record of the study and evaluation of the internal controls related to the information system.
    - Copies of audit reports and observations of earlier years.
    - Copies of management letters issued by the auditor, if any
  - Current Audit Files: CAF which contain information relating **PRIMARILY TO AUDIT OF A SINGLE PERIOD**. The current file normally includes:
    - Correspondence relating to the acceptance of appointment and the scope of the work.
    - Evidence of the planning process of the audit and audit programme.
    - A record of the nature, timing, and extent of auditing procedures performed, and the results of such procedures.
    - Copies of letters and notes concerning audit matters communicated to or discussed with the client, including material weaknesses in relevant internal controls.
    - Letters of representation and confirmation received from the client.
    - Conclusions reached by the auditor concerning significant aspects of the audit, including the manner in which the exceptions and unusual matters, if any, disclosed by the auditor's procedures were resolved and treated.
    - Copies on the data and system being reported on and the related audit reports.

- **WORKING PAPERS ARE THE PROPERTY OF THE AUDITOR**.
- The auditor may, at his discretion, make portions of, or extracts from his working papers available to the client.
- The auditor should
  - Adopt reasonable procedures for **CUSTODY AND CONFIDENTIALITY** of his working papers and
  - Retain them for a period of time sufficient to meet the needs of his practice and satisfy any pertinent legal and professional requirements of record retention.

- Planning the Documentation: It is important to understand why it is important to plan

documentation. The following three parameters would help in planning a documentation process.

I. The importance of planning and understanding the planning process requires identifying three planning questions:
   - ✳ Knowing Your Resources:
     - The three basic resources: time, people, money.
     - One has to check for their availability and affordability.
   - ✳ Defining the Scope and Audience:
     - The same report may undergo significant changes depending on the character of report and nature of audience.
     - Presentation on Balance Sheet made to bankers and to investors would be quite different in content and focus.
   - ✳ Using a Scope Definition Report:
     - It is critical to know how to complete a Scope Definition Report.
     - This report helps in developing a workable schedule for completing the project.

II. The Documentation Writer: The qualities and skills that the documentation writer would need. The requirement may often be legal in nature

III. Rules to guide documentation writing

To get a good documentation of the working papers of an auditor, what are the point to be considered while gathering and organizing information and also mention the principle to be followed for writing the documentation? (N'10- 8 Marks)

- ☞ Gathering Information: To be able to have a good documentation, it is necessary to get information about the reader and the requirement of the document.
  - ✳ About the Reader:
    - Finding information about the reader by doing a task analysis.
    - Three parts of the task: viz. input, process, output will have to be identified before one could develop an understanding of a reader.
  - ✳ About the Subject: The three sources of information about a subject are people, paper, and the object of the report.

- ☞ Organizing Information:
  - ✳ Organizing information involves deciding what information to include and how to sequence it.
  - ✳ This covers five organizational sequences and examines how to divide the documentation into various sections and subsections.
    - 🖋 Selecting Information:
      - Selecting 'what the reader needs to know'.
      - Organizing the information into a useful sequence.
    - 🖋 Organizing the Documentation: Using the five organizational sequences: subject, difficulty, chronological, importance and analytical.
    - 🖋 Dividing Into Sections: Dividing documentation into chapters or sections.
    - 🖋 Dividing Into Subsections: Dividing sections or chapters into subsections.

- Writing the Documentation: Writing is governed by the following major rules/principles:
  - Writing in Active Voice: Using active voice in documentation.
  - Giving the Consequences: Giving the consequences of the reader's action.
  - Writing from General to Specific: Designing the documentation from general to specific.
  - Consistency: Using style, order and format consistently.
  - Writing Online Documentation: Laying down guidelines for writing online documentation.
- Finalizing Documents: This section identifies the tasks involved in reviewing and testing the document, generating the glossary and index and formatting the document for final production.
  - Reviewing and Testing:
    - Selection of reviewer of the documentation involves identification of subject and communication skill.
    - The reviewer must be provided with adequate information regarding the audience and object of the report.
    - In order to ensure objectivity it is recommended that the reviewer be a person who has not been involved in the documentation process.
  - Generating the Glossary and Index:
    - Compilation of a glossary and generation of an index are two major tasks for a complete documentation.
    - In order to achieve this task it is necessary to mark the Index and glossary entries at the stage of documentation itself.
    - Word processing software comes with an inbuilt ability of creating an index from the identified text in the body of the document.
  - Formatting and Production:
    - The idea of creating a good document is incomprehensible without first deciding on a good design for the same.
    - This involves choosing effective formatting options for headings, sub-headings, section breaks, formatting, and allied.
    - It also important to select an appropriate binding style that would aid filing and ease of consultation.

⇨ IS AUDIT REPORT (M'11- 8 Marks)

- IS Audit reports broadly include the following sections: title page, table of contents, summary including the recommendations, introduction, findings and appendices.
- These components of an audit report are discussed below:

1. Cover and Title Page:
   - Audit reports should use a standard cover, with a window showing the title: "Information System Audit" or "Data Audit", the department's name and the report's date of issue (month and year).
   - These items are repeated at the bottom of each page.
   - The title page may also indicate the names of the audit team members.
2. Table of Contents: The table lists the sections and sub-sections with page numbers including summary and recommendations, introduction, findings (by audit field) and

appendices (as required).

3. Summary / Executive Summary:
   - ✳ The summary gives a quick **OVERVIEW OF THE SALIENT FEATURES** at the time of the audit in light of the main issues covered by the report.
   - ✳ It should not normally **EXCEED THREE PAGES**, including the recommendations.
4. Introduction:
   - ✳ Since readers will read the summary, the introduction should **NOT REPEAT DETAILS**.
   - ✳ It should include the following elements:
     - Context:
       - This sub-section briefly describes conditions in the audit entity during the period under review.
       - For instance,
         - the entity's role,
         - size and organization especially with regard to information system management,
         - significant pressures on information system management during the period under review,
         - events that need to be noted, organizational changes,
         - IT disruptions,
         - changes in roles and programs,
         - Results of internal audits or follow-up to our previous audits, if applicable.
     - Purpose: This sub-section is a short description of what functions and special programs were audited and the clients' authorities.
     - Scope: The scope lists the period under review, the issues covered in each function and program, the locations visited and the on-site dates.
     - Methodology:
       - This section briefly describes sampling, data collection techniques and the basis for auditors' opinions.
       - It also identifies any weaknesses in the methodology to allow the client and auditee to make informed decisions as a result of the report.
5. Findings:
   - ✳ Findings constitute the **MAIN PART OF AN AUDIT REPORT**.
   - ✳ They result from the examination of each audit issue in the context of established objectives.
6. Opinion: If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in **CONSONANCE** to the requirement.
7. Appendices:
   - ✳ Appendices can be used when they are **ESSENTIAL FOR UNDERSTANDING THE REPORT**.
   - ✳ They usually include comprehensive statistics, quotes from publications, documents, and references.