

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

BASIC CONCEPTS

1. Information System Security:

Security 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, and insurance is commonly understood and implemented by most organizations.

1.1 Security Objective: For any organization, the security objective comprises three universally accepted attributes:

Confidentiality: Prevention of the unauthorized disclosure of information.

Integrity: Prevention of the unauthorized modification of information.

Availability: Prevention of the unauthorized withholding of information.

1.2 Sensitive Information: The sensitive information is: Strategic Plans, Business Operations, and Finances.

1.3 Establishing better Information Protection: The major points to be considered are: Not all data has the same value, Know where the critical data resides, Develop an access control methodology, Protect Information stored on media, Review hardcopy output.

2. Preventive Information Protection: This type of protection is based on use of security controls. Information system security controls are generally grouped into three types of control: Physical, Logical, and Administrative. Organizations require all three types of controls.

3. Information Security Policy: 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.

3.1 Members of Security Policy: Security has to encompass managerial, technological and legal aspects. Security policy broadly comprises the following three groups of management: Management members who have budget and policy authority, Technical group who know what can and cannot be supported, and Legal experts who know the legal ramifications of various policy charges.

4. Types of Information Security Policy: Various policies are: Information Security Policy, User Security Policy, Acceptable Usage Policy, Organizational Information Security Policy, Network and System Security Policy, Information Classification Policy, Conditions of Connection.

4.1 Components of 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, Identity Management and access control, IT Operations management, IT Communications, System Development and Maintenance Controls, Business Continuity Planning, Legal Compliances, Monitoring and Auditing Requirements, and Underlying Technical Policy.

5. Audit Policy: Purpose of this audit policy is to provide the guidelines to the audit team to conduct an audit on 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 attacks, Open ports, which may be accessed from outsiders, and Unrestricted modems unnecessarily open ports. Audits may be conducted to ensure integrity, confidentiality and availability of information and resources.

5.1 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. 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, and People.

- 6. IS Audit Reports:** Audit reports broadly include the following sections: title page, table of contents, summary (including the recommendations), introduction, findings and appendices. The 'Introduction' section includes: Context, Purpose, Scope, Methodology, Findings, Opinion, and Appendices.

Question 1

Discuss various types of Information Security policies and their hierarchy.

Answer

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.

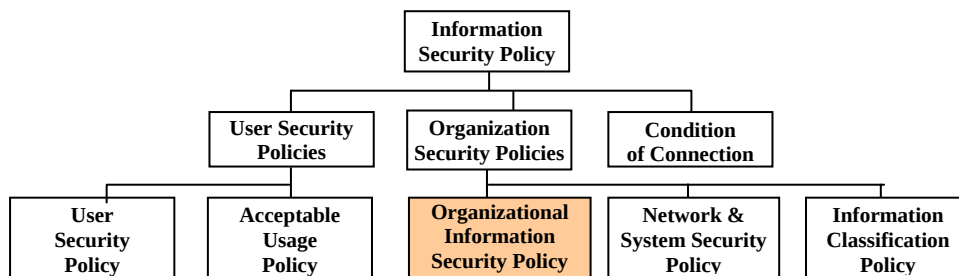


Fig: The hierarchy of Information Security Policies

Question 2

State and briefly explain the contents of a Standard Information System Audit Report.

Answer

According to the recommendations, 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:

- (i) *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.
- (ii) *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).
- (iii) *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.
- (iv) *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.

- (v) *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.
- (vi) *Opinion*: If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in consonance to the requirement.
- (vii) *Appendices*: Appendices can be used when they are essential for understanding the report. They usually include comprehensive statistics, quotes from publications, documents, and references.

Question 3

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.”

Answer

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

Information Systems Control and Audit

- reference to supporting documentation.

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 policy may be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organization. In general, most if not all employees covered by the ISMS scope will have some responsibilities for information security, and 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:

- (i) Definition of information security,
- (ii) Reasons why information security is important to the organization,
- (iii) A brief explanation of the security policies, principles, standards and compliance, and
- (iv) Reference to supporting documents.

Question 4

What purpose the information system audit policy will serve? Briefly describe the scope of information system audit.

Answer

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 attacks
- Open ports, which may be accessed by outsiders
- Unrestricted modems, unnecessarily open ports

Audits may be conducted to ensure integrity, confidentiality 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. Such evaluation, in the aggregate, provides information to 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 Systems Control and Audit

- Information system budget and monitoring of variances.
- High level policies for information system use and the protection and monitoring of compliance with these policies.
- 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 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.

Question 5

You have been asked to conduct an I.S. Audit for a bank. (i) How will you develop a documented audit program? (ii) What kind of working papers and documentation you will prepare?

Answer

- (i) The **documented audit program** is developed with the help of following activities:
- Documentation of the IS auditor's procedures for collecting, analysing, interpreting, and documenting information during the audit.
 - Objectives of the audit.
 - Scope, nature, and degree of testing required to achieve 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.
- (ii) **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.

In case of recurring audits, some working paper files may be classified as permanent audit files which are updated currently with information of continuing importance to succeeding audits, as distinct from the current audit files which contain information relating primarily to audit of a single period.

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.

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.

Information Systems Control and Audit

- 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 should 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.

Question 6

Explain the basic types of Information Protection that an Organization can use.

Answer

Types of Information Protection: 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.

Preventative Information Protection: It is based on use of security controls, which itself is a group of three types of controls such as Physical, Logical, and Administrative.

- *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.

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. Hence, the key requirement of any restorative information system protection plan is that the information systems can be recovered. The claim of back program to backup data automatically cannot be

reliable. It has so many problems. 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.

Question 7

Describe the role of information systems audit policy in ensuring information security with respect to:

- (i) Scope of IS Audit
- (ii) Purpose of IS Audit

Answer

- (i) **Scope of IS Audit:** The IS audit policy is to provide the guidelines to the audit team to conduct an audit on IT based infrastructure system in ensuring information security are:

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. Such evaluations, in the aggregate, provide information to 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.

Information Systems Control and Audit

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 others, 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 budgets and monitoring of variances.
- High level policies for information system use and the protection and monitoring of compliance with these policies.
- 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 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.

(ii) **Purpose of IS Audit:** Purpose of this audit policy is to provide the guidelines to the audit team to conduct an audit on 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 attacks
- Open ports, which may be accessed from outsiders
- Unrestricted modems unnecessarily open ports

Audits may be conducted to ensure integrity, confidentiality 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
- Maintenance 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.

Question 8

Briefly discuss the issues addressed under the following headings in an information systems (IS) audit Security policy document.

- (i) *Responsibility Allocation*
- (ii) *Asset and security Classification*
- (iii) *Access Control*
- (iv) *Incident Handling*

Answer

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.

- (i) **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.

Information Systems Control and Audit

- 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
- (ii) 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. 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.
 - Appropriate procedures for information labeling and handling must be agreed and put into practice.
 - Classified waste must be disposed of appropriately and securely.

(iii) 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.

(iv) 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

Question 9

What are the various types of Information Security Policies? What are the hierarchical relationships between these policies? Discuss briefly.

Answer

Types of Information Security Policies and their Hierarchy:

- ◆ *Information Security Policy: This policy provides a definition of Information Security, its overall objective and the importance applies to all users.*
- ◆ *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.*
- ◆ *Acceptance Usage Policy: This sets out the policy for acceptance use of e-mail and internet services.*
- ◆ *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.*
- ◆ *Network and System Security Policy: This policy sets out detailed policy for system and network security and applies to IT department users.*
- ◆ *Information classification policy: This policy sets out the policy for the classification of information.*
- ◆ *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 supplies systems.*

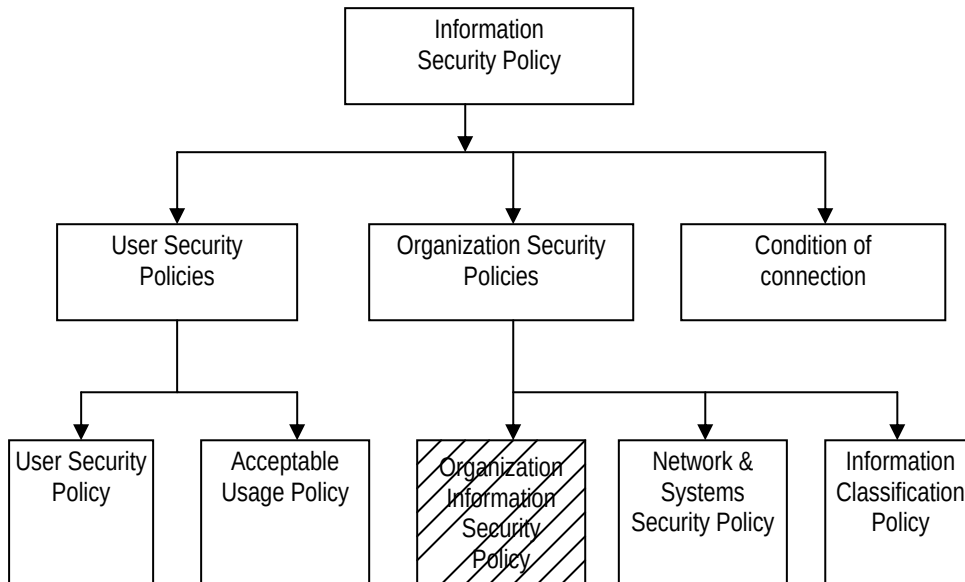


Fig. : The hierarchy of Information Security Policies

Question 10

What are the components of the Security Policy?

Answer

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.

Information Systems Control and Audit

- ◆ System development and maintenance controls.
- ◆ Business continuity planning.
- ◆ Legal compliances.
- ◆ Monitoring and Auditing Requirements.
- ◆ Underlying technical policy.

Question 11

What is meant by physical and environmental security?

Answer

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.

Question 12

What is meant by SYSTRUST and WEBTRUST? Discuss in brief.

Answer

SYSTRUST and WEBTRUST: Systrust and Webtrust are two specific services developed by the AICPA that are based on the trust services principles and criteria. Systrust engagements are designed for the provision or advisory services or assurance on the

reliability of a system. Webtrust engagements relate to assurance or advisory services on an organization. System related to e-commerce. Only Certified Public Accountants (CPAs) may provide the assurance services of trust services that result in the expression of a trust services, webtrust, or systrust opinion and in order to issue systrust or webtrust reports, CPA firms must be licensed by the AICPA.

The following principles and related criteria have been developed by the AICPA/CICA for use by practitioners in the performance of Trust services engagements such as systrust and webtrust.

- ◆ *Security*: The system is protected against unauthorized access (both physical and logical).
- ◆ *Availability*: The system is available for operation and use as committed or agreed.
- ◆ *Processing integrity*: System processing is complete, accurate, timely and authorized.
- ◆ *On-line privacy*: Personal Information obtained as a result of e-commerce is collected, used, disclosed and retained as committed or agreed.
- ◆ *Confidentiality*: Information designated as confidential is protected as committed or agreed.

Each of these principles and criteria are organized and presented in four broad areas:

- ◆ *Policies*: The entity has defined and documented its policies relevant to the particular principle.
- ◆ *Communications*: The entity has communicated its defined policies to authorized users.
- ◆ *Procedures*: The entity uses procedures to achieve its objectives in accordance with its defined policies.
- ◆ *Monitoring*: The entity monitors the system and takes action to maintain compliance with its defined policies.

Question 13

ABC Technologies is a leading company in the BPO sector. Its most of the business processes are automated. The company is relying on Information Technology for information and transaction processing. The growth of E-commerce supported by the growth of the Internet has completely revolutionized and reengineered business processes. The company's new business models and new methods presume 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. However, in reality, the technology-enabled and technology-dependent organizations are more vulnerable to security threats than ever before.

Read the above carefully and answer the following:

- (a) Discuss the security objective of the organization.*
- (b) There are certain basic ground rules that must be addressed sequentially, prior to know the details of 'how to protect the information systems'. Explain those rules in brief.*
- (c) Describe various groups of management, comprised by security policy.*

Answer

- (a) Security Objective :** The objective of information system security is “the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of confidentiality, integrity, and availability”.

For any organization, the security objective comprises three universally accepted attributes:

- Confidentiality: Prevention of the unauthorized disclosure of information.
- Integrity: Prevention of the unauthorized modification of information.
- Availability: 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.

- (b)** 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.) '
- (c)** Security has to encompass managerial, technological and legal aspects. Security policy broadly comprises the following three groups of management:

- Management members who have budget and policy authority,
- Technical group who know what can and cannot be supported, and
- Legal experts who know the legal ramifications of various policy charges.

Information security policies must always take into account business requirements. Business requirements are 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. The respect of intellectual property is a good example of such requirements.

EXERCISE

Question 1

An organization is committed to implement the information security policy through established goals and principles. The major problem, organization is facing through its employees. There is neither any proper allocation of duties/ responsibilities between employees nor a proper reporting hierarchy. Suggest a proper security organization structure and responsibility allocation, to come out of these problems.

Question 2

An Information Systems Audit Report contains various components: Cover and title page, Table of contents, Summary/Executive summary, and Appendices. But after submission, the principal auditor raised the query that the report is not correct as it missed various important components. Explain the missing components in brief.

Question 3

An Information System Audit Report includes various sections: Title Page, Table of Contents, Summary, Introduction, Findings and Appendices. Explain various elements, included in the 'Introduction' section.

Question 4

It is clear from various instances that there are not only many direct and indirect benefits from the use of information systems, but also many direct and indirect risks related to the use of information systems. These risks have led to a gap between the need to protect systems and the degree of protection applied. Briefly explain the causes of this gap.

Question 5

Briefly discuss end user computing policies with respect to a sample IS Security Policy.

Question 6

Differentiate between the responsibilities of a Facilities Management Security Officer and Divisional System Security Officer with respect to the organizational security structure.