

DRAFTING OF IS SECURITY POLICY, AUDIT POLICY, IS AUDIT REPORTING – A PRACTICAL PERSPECTIVE

Question 1

Discuss various types of Information Security policies and their hierarchy. (5 Marks) (Nov 2008)

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. *Organisational 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.

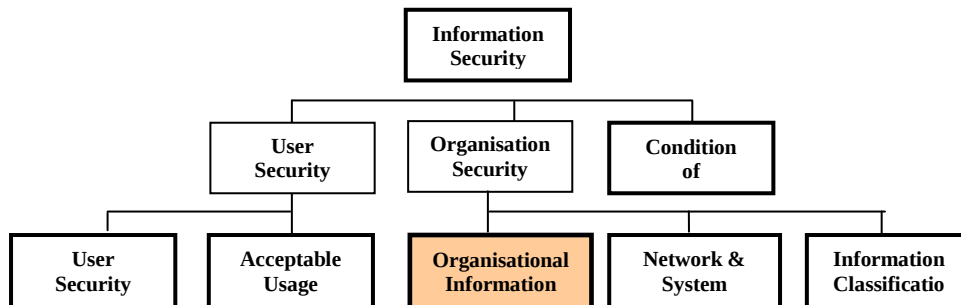


Fig. : The hierarchy of Information Security Policies.

Question 2

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."

Identify the salient components that have not been covered in the above policy.

(5 Marks) (Jun 2009)

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
- 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 3

What purpose the information system audit policy will serve? Briefly describe the scope of information system audit.
(10 Marks) (Jun 2009)

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 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 4

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?
(10 Marks) (Nov 2009)

Answer

(i) The documented audit program is developed as given below:

- .. 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 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; and
- .. 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;

- .. 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; and
- .. 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 5

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

(5 Marks) (Nov 2009)

Answer

Types of Information Protection: The two basic types of information protection that an organization can use are:

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

These are discussed below, one by one;

1. **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.
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. 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 tested recently?

- .. The time taken for restoration,
- .. The quantum of productivity loss,
- .. The strict adhere of plan, and
- .. The time needed to input the data changes since the last backup.

Question 6

What are the aspects to be included when a documented audit program is developed?

(4 Marks) (Nov 2010)

Answer

A documented audit program would include the following aspects:

- (i) Documentation of the information system auditor's procedures for collecting, analyzing, interpreting and documenting information during the audit;
- (ii) Objectives of the audit;
- (iii) Scope, nature and degree of testing required achieving the audit objectives in each phase of the audit;
- (iv) Identification of technical aspects, risks, processes and transactions, which should be examined; and
- (v) Procedures for audit will be prepared prior to the commencement of audit work and modified, as appropriate, during the course of the audit.

Question 7

To get a good documentation of the working papers of an auditor, what are the points to be considered while gathering and organizing information and also mention the principles to be followed for writing the documentation?

(8 Marks) (Nov 2010)

Answer

In order to get a good documentation of the working papers of an auditor, the following points are to be considered during gathering information:

- (i) *About the reader:* Finding information about the reader by doing a task analysis. Three parts of the task viz. input, process, and output will have to be identified before one could develop an understanding of a reader.
- (ii) *About the subject:* The three sources of information about a subject are people, paper and the object of the report.

Organizing information:

The points to be considered during organizing information are given as under:

- (i) *Selecting Information*: Selecting 'what the reader needs to know', organizing the information into a useful sequence.
- (ii) *Organizing the documentation*: Using the five organizational sequences: subject, difficulty, chronological, importance and analytical.
- (iii) *Dividing into sections*: Dividing documentation into chapters or sections.
- (iv) *Dividing into subsections*: Dividing sections or chapters into subsections.

Principles for writing the documentation:

Following principles should be kept in mind for writing the documentation:

- *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; and
- *Writing online documentation*: Laying down guidelines for writing online documentation by using appropriate techniques to emphasize text.

Question 8

As an IS Auditor, discuss the various contents in brief to be included in a standard audit report.
(8 Marks) (May 2011)

Answer

An Audit report includes the following sections: title page, table of contents, summary (including recommendations), introduction, findings and appendices.

These are discussed below:

- *Cover and Title Page*: Audit reports should use a standard cover page, with a window showing the title "Information System Audit" or "Data Audit", the department's name and the report's date of issue. These items are repeated at the bottom of each page. The title page may also indicate the names of the audit team members.
- *Table of contents*: The table lists the sections and subsections with page numbers including summary and recommendations, introduction, findings and appendices.
- *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 exceed three pages, including recommendations.

- **Introduction:** It should include the following elements:
 - Context: This subsection briefly describes conditions in the audit entity during the period under review, for instance, the entity's role, size and organization 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 subsection is a short description of what functions and special programs were audited and the client's 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 auditor's options. It also identifies any weakness/es in the methodology to allow the client and auditee to make informed decisions as a result of the report.
- **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 and client's expectations. If the auditor is using any standard grading, the arrived value should also be stated.
- **Opinion:** If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in consonance to the requirement.
- **Appendices:** Appendices can be used when they are essential for understanding the report. They usually include comprehensive statistics, quotes from publications, documents, and references.