

## **9. Drafting of IS security Policy, Audit Policy, IS Audit Reporting – A Practical Perspective**

### **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.

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.

Security objective: the objective of security information system is “the protection of the interests of those relying in information, and the information systems and communications that deliver the information, from harm resulting from failures of confidentiality, integrity and availability.” This may be classified universally as follow for any organization

1. Confidentiality: prevention of the unauthorized disclosure of information
2. Integrity: prevention of the unauthorized modification of information
3. Availability: prevention of the unauthorized withholding of information.

### **What information is sensitive?**

1. Information related to Strategic plan of the company
2. Business operations
3. Finances

### **Steps for to do for protection of information**

Protecting the information is crucial to the overall success or failure of company. For protecting such information they should consider the following point.

1. Not all data has the same value: and as such information may be handled and protected differently. Organizations must determine the value of the different types of information in their environment before they can plan for the appropriate levels of protection.
2. Know where the critical data resides: in today's business environment, this is normally the company/s information system infrastructure
3. Develop an access control methodology: information does not have to be removed to cause damage or to have financial impact. To guard information against fraud, organizations must establish some type of access control methodology.
4. Protect information stored on media: companies should control magnetic media to reduce the loss of software. And finally, when migrating from one platform to another, the status of all hard drives and the associated data should be controlled.
5. Review Hand copy output

### **Protecting Computer-Held information systems**

Prior to discussing the details of ‘how to protect information system’ we need to define a few basic ground rules that must be addressed sequentially:

- a. We need to know that ‘what is information systems are’ and ‘where these are located’
- b. We need know the value of the information held and how difficult it would be to recreate if it were damaged or loss.
- c. We need to know that ‘who is authorized to access the information’ and ‘what they are permitted to do with the information’
- d. We need to know that ‘how quickly information needs to be made available should and it become unavailable for whatever reson.

There are two basic types of protection that an organization can use.

1. Preventive Information protection: this type of protection is based on use of security controls. Information system security control is generally grouped into three type of control.
  - a. Physical
  - b. Logical (technical)
  - c. Administrative
2. Restorative Information Protection: planning and operating an effective and timely information system backup and recovery program is vital to an operation. The key requirement of any restorative information system protection plan is that the information system can be recovered. This is frequently an issue that many organization fail to properly address.

### **Holistic protection**

Protecting corporate information system from harm or loss is not an easy task. Protection must be done holistically and give the organization the appropriate level of security at a cost that is acceptable to the business. One must plan for the unexpected and unknown, expect that the worst event to happen, and recover from these events if and when they occur, as through nothing ever happened.

### **Information Security Policy**

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 privilege, separation of duties, who controls and who owns the information, and authority issues.

### **Types of Information security policies and their hierarchy**

- Information security policy: it provides a definition of information security, its overall objective and the importance to all users
- User security policy: this policy sets out the responsibilities and requirements for all IT system Users.
- Acceptable usage policy: this sets out the policy for acceptable level use of email 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 system processing this information.
- Network & 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.
- Condition of connection: this policy sets out the group policy for connecting their network.

### **Components of the security policy**

- 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
- Underlying technical policy

### **Purpose and Scope of IS policy**

- a. Deny authorized access to any IT resources and restrict access to data and resource or IT processes.
- b. Within the operational constraints, the security controls will allow the required service to be available to authorized users only.
- c. The scope define how far the policy would be applicable, ti whom it would be applicable and the period for which the policy would be applicable

### **Security Organization structure**

The security responsibility and the line of reporting in the organization should be deifned in the policy as stated below

1. Information system forum
2. Information security management group
3. Group security officer
4. Assistant group security officer
5. IT management
6. IT security officer
7. Installation security officer
8. Personnel security officer
9. Facilities management security officer
10. Divisional system security officer
11. System security officer
12. System owners
13. Line mangers
14. Users

### **Incident handling**

For incident handling, following are the major points

- 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 weakness or trends
- Procedures for the collection of evidences relating to security incidents should be standardized. All staff must be made aware of the process. Adequate records must be maintained and inspections affiliated to enable the investigation of security breaches or concerted attempts by third parties to identify security weakness.

### **Audit Policy**

#### **➤ Purpose**

Purpose of this audit policy is to provide the guidelines to the audit team to conduct an audit on IT based infrastructure system. The IS audit policy should be lay out the objective and the scope of the policy. an IS audit is conducted to

- Safeguard the information system assets/resources
- Maintain the data integrity
- Maintain the system effectiveness
- Ensure system efficiency; and

- Comply 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.  
 The scope of the audit will also include the internal control system for the use and protection of information and the information system.

### **What Audit policy should do?**

- The policy should layout the periodicity of reporting and the authority to whom the reporting is to be made
- A statement of professional proficiency may be included to state the minimum qualification and experience requirements of the auditors.
- All information system auditors will sign a declaration of fidelity and secrecy before commencing the audit work in a form that the inspection department may design
- The policy may lay out the extent of testing to be done under various phases of the audit planning, compliance testing, substantive testing
- Documentation of the information system auditor's procedures for collecting, analyzing, interpreting and documenting information during the audit.
- The policy should determine when and to whom the audit results would be reported and communicated.
- The policy should outline the compliance testing areas e.g. organizational and operational control, security management control, system development and documentation control, access control etc.
- The auditor will carry out substantive testing wherever the auditor observes weakness in internal control or where risk exposure is high.
- The audit policy would define the compulsory audit working papers to be maintained and their formats.

### **Audit Working paper and documentation**

- The permanent audit file includes
  1. The organizational structure of the entity
  2. The IS policies of the organization.
  3. The historical background of the information system in the organization.
  4. Extracts of copies of important legal documents relevant to audit
  5. a record of the study and evaluation of the internal control related to information system,
  6. copies of audit reports and observation of earlier years,
  7. copies of management letters issued by the auditor, if any
- **The Current file normally includes**
  1. Correspondence relating to the acceptance of appointment and the scope of the work,
  2. Evidence of the planning process of the audit and audit programmed,
  3. A record of the nature, timing and extent of auditing procedures performed, and the results of such procedures.
  4. Copies of letters and notes concerning audit matters communicated to or discussed with the client, including material weakness in relevant internal control.
  5. Letters of representation and confirmation received from the client.
  6. 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

7. Copies on the data and system being reported on and the related audit papers.

### **IS Audit Reports**

- i. cover and title page: showing the title 'Information system Audit' or 'data audit'
- ii. Table of contents
- iii. Summary/Executive summary: it gives a quick overview of salient features at the time of audit in light of the main issues covered by the report.
- iv. Introduction:
  - a. Context
  - b. Purposes
  - c. Scope
  - d. Methodology
- v. Findings
- vi. Opinion
- vii. Appendices

### **Level of Detail:**

The depth of coverage of issues should be normally reflecting the significance of the findings. Situations representing a high degree of risk or indicting shortcomings that are serious enough to justify recommendations should be treated extensively.

### **Commentary:**

Where recommendations and complaints are made under the same issue, they should be in separate paragraphs; otherwise they may confuse the reader and reduce the impact of one of the other.

Statistics need to be used consistently throughout the report.

Percentage should not be used when referring to small samples.

Graphics should be used when they add to the understanding of the text.