

In today's parlance business processes are automated, organizations are increasingly relying on information technology which is again supported by growth of E-commerce. All these new business models presume that the information required by managers is accurate, reliable and all the time available further virtual business are running all the time on 24 \* 365 hrs basis. However, in reality, the technology dependent organizations are more exposed to security threats than ever before, therefore they need to provide more information security than before.

**9.1 Why Information Security is important :-**

- In a global information society the importance of information is very critical.
- Organizations depends on timely, accurate, complete, valid, consistent, relevant and reliable information.
- Management has a responsibility to ensure that the organization provides all users with a secure information system environment.
- There are not only many benefits from the use of information system but also many risks involved.
- These risks have led to a gap between the need to protect system and the degree of protection applied. This is due to -
  1. Widespread use of technology
  2. Interconnectivity of system
  3. Elimination of distance, time, and space as constraints.
  4. Rapid technological changes
  5. Decrement in mgmt and control
  6. Increase in unconventional electronic attaches.
  7. External factors such as regulatory requirements
- Security failure may result in both financial and/or intangible losses.
- Threats to information system may arise from intentional or accidental act, may come from internal and external sources, and may be of any of the following form -
  1. Technical conditions                      -    program bug, disk crashes
  2. Natural disaster                            -    fire, flood
  3. Environmental conditions                -    short circuits
  4. Human factors                              -    lack of training, negligence
  5. Unauthorised access                      -    hacking
  6. Virus

**9.2 What is Information Security :-**

Information security relates to the physical and logical protection of data or information recorded, processed, shared, transmitted or received from an electronic form. The protection is provided against loss, inaccessibility, alteration, or unauthorised disclosure. The protection is achieved through physical safeguard such as locks, security guard, insurance etc and logical safeguard such as user identifiers, passwords, firewalls etc.

**9.2.1 The objective of information security**

"The protection of the interest of those relying on information, information system and communication that deliver the information from harm resulting from failure of availability, confidentiality and integrity."

The security objective can be achieved by ensuring -

**Availability** - System is available when required.

**Confidentiality** - Information is accessible to only authorised person.

**Integrity** - Information is protected against unauthorised modification.

**9.2.2 Sensitive information**

Sensitive information which requires security includes the following -

**(a) Strategic plan** Strategic plans shape future of the organization. It is the organization foresighted by top management. They are very crucial to the success of the organization.

**(b) Business operation** It consists of organizations process and procedure. They may provide a market advantage in the case when one organization can provide a service profitably at a lower price.

**(c) Finance** Salaries and wages, cost of production, material cost etc are very sensitive and should not be leak out.

**9.2.3 Factors for establishing better information protection**

The following points should be considered while providing protection to the information

- *Not all data has the same value* : Organizations must determine value of the information before planning the level of protection to be provided to that information.
- *Know where the critical data resides*: Every place of information requires different level of information protection therefore identifying where information is located is essential for developing security plan. Centralised storage system, De-centralized storage system, Network system etc suggest type of security solution required.

- Develop an access control methodology: Access control methodology makes it difficult for intruder to gain unauthorised access of vital information thereby enhances the security level. It is due to fact that information damage does not always mean deletion of information, it may be caused by unauthorised access, copy or modification.
- Protect information stored on media: Information available on-line is of course more exposed to risk of damage or theft but information stored on media needed same amount of protection as computer storage media are easily portable.
- Review hardcopy output: The hardcopy of the employee's daily work should be reviewed. Confidentiality should be maintained during distribution of hardcopy reports.

### 9.3 **Protecting computer - Held information :-**

#### 9.3.1. **Basic rules -**

Before deciding about how to protect the information held electronically. There are some basic ground rules that must be addressed sequentially -

- Rule # 1 : First ascertain what the information is and where it is located.
- Rule # 2 : Determine the value of information and difficulty in re-creating it.
- Rule # 3 : Determine who is authorised to access the information and what they are permitted to do.
- Rule # 4 : Determine how quickly information is needed.

#### 9.3.2. **Protection -**

There are 3 basic types of protection provided to computer held information -

##### **(a) Preventative Protection -**

This type of protection is based on use of security controls. Information system controls are grouped into 3 categories -

- Physical - Doors, Locks, Guards, floppy disk access lock, CCTV.
- Logical - Passwords, Access privileges, Power protection system.
- Administrative - Security awareness, user A/C revocation policy.

##### **(b) Restorative Protection -**

Events that damage information happens inspite of many security arrangements. If an organization cannot recover in an acceptable time period, it can go out of business. Planning and operating an effective and timely information backup and recovery program provides restorative protection to information. However, some major issues to be addressed are -

- Has the recovery process tested periodically
- How long did it take to recover information
- How much productivity will be lost.
- Did everything go according to the plan.
- How much time it takes to take backup.

##### **(c) Holistic Protection -**

Protection must be done holistically & give the organization the appropriate level of security at a reasonable cost & should not damage the interest of the people.

#### 9.4 Information Security Policy :-

A policy is a plan or course of action, designed to influence decision, 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 concern, who may access what information and in what matter, maximised sharing versus least privilege, separation of duties, who controls and who owns the information etc.

##### 9.4.1 Issues to address

The IS policy state senior management's commitment to information security. It should at least address the following issues:

- A definition of information security,
- Reasons why information security is important to the organization, and its goal and principles,
- A brief explanation of the security policies, principles, standards and compliance requirement,
- Definition of all relevant information security responsibilities,
- Reference to supporting documentation.
- IS policy must always take into account business requirements. E-commerce security is an example of such business requirement.
- Policy must consistently take into account the legal, statutory, regulatory and contractual requirement.

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 content.

##### 9.4.2 Members of Security Policy

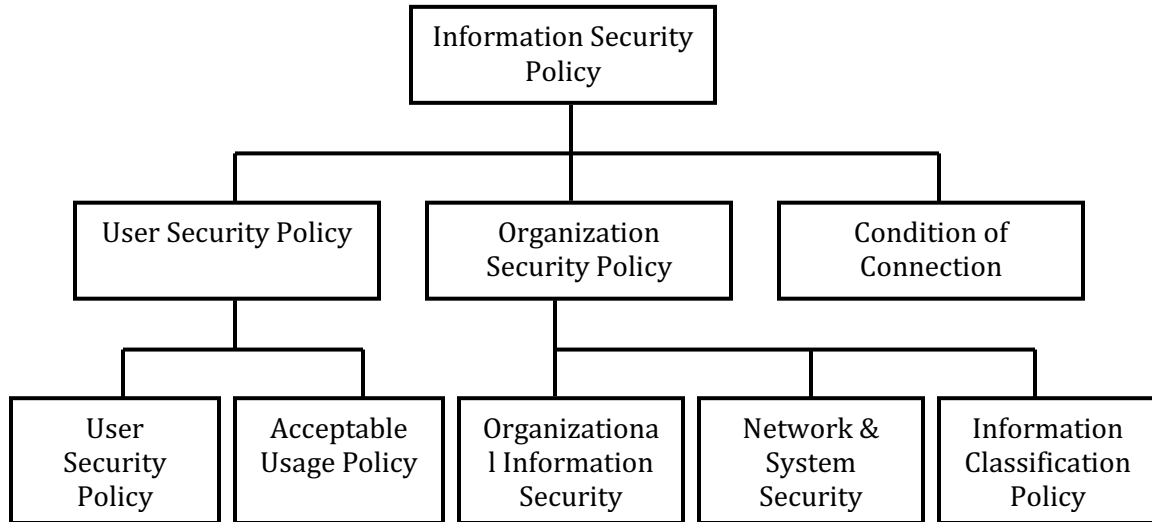
Security policy broadly comprises the following three groups of management:

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

#### 9.5 Types of IS Policy and their Hierarchy :-

- **Information Security Policy** - It defines Information security, its overall objectives and importance.
- **User security policy** - This policy sets out the responsibilities and requirements for all IT systems users.
- **Acceptable Usage Policy** - This sets out the policy for acceptable use of email and internet services.

- **Organization Information Security Policy** - This policy set out security of information assets and the information technology(IT) systems. It is the main security policy document.
- **Network & system policy** - This policy sets out detailed policy for system and network security.
- **Information classification policy** - This policy set out the policy for the classification of information.
- **Condition of connection** - This policy sets out the group policy for connecting to their network.



***Hierarchy of Information Security Policies***

## **9.6 Components of the Security Policy**

A good security policy should clearly state the following

- Purpose and scope of the security and the intended audience
- The Security infrastructure
- Security policy document updation and compliance requirements
- Incident response mechanism and incident reporting
- Security organization structure
- Inventory and classification of assets
- Description of technologies
- Physical and environmental security
- Identity Management and access control
- IT Operation management
- IT Communications

- System Development and Maintenance Controls
- Business Continuity Planning
- Legal Compliances
- Monitoring and Auditing Requirements
- Underlying Technical Policy

**9.7 Purpose and Scope**

The primary objective of the policy would be to ensure confidentiality, integrity and availability of information and related systems. The security policy is designed to -

- a) Deny unauthorised access of any IT resources
- b) Within the operational constraints, the security control will allow the required services to be available to authorised users only.
- c) The scope defines how far the policy would be applicable.

**9.8 Security Organization Structure**

The security responsibility and the line of reporting in the organization should be defined as below -

- [1] Information security Forum (ISF) :** This forum is chaired by the GSO and includes senior representative from each of the divisions within the group, together with the AGSO. It is the role of this forum to ensure that there is clear direction and visible management support of security initiative within the organization.
- [2] Information Security Management Group (ISMG):** This cross functional group is chaired by the AGSO and comprises of a Divisional System Security Officer(DSSO) from each of the division, together with the IT security officer, and personnel and facilities management security officers. Its role is to co-ordinate the implementation and management of information security control across all of the division and sites.
- [3] Group security officer (GSO):** The GSO will have overall responsibility for security within the group. This includes the security of all information assets, the network accreditation scheme and non-IT security.
- [4] Assistant Group Security Officer (AGSO) :** The AGSO reports to the GSO and the information security forum and is responsible for the co-ordination of-information security implementation and management across the group.

- [5] **IT Management:** IT management have overall responsibility for security of the IT infrastructure. This is discharged mainly through installation security officers and the IT security officer.
- [6] **IT Security Officer (ITSO) :** The ITSO reports to the ISMG. The ITSO is responsible for managing IT security programmes and IT security incidents.
- [7] **Installation Security Officer (ISO) :** An ISO will be appointed for each IT environment from the IT team leaders. ISO will be responsible for all security matters related to their system/installation and network.
- [8] **Personnel Security Officer (PSO):** The PSO will report directly to personnel management on all security matters relating to personnel. The role involves ensuring the controls set out are implemented, adhered to and reviewed as necessary.
- [9] **Facilities Management Security Officer (FMSO) :** The FMSO will report directly to facilities management on all security matters relating to personnel. The role involves ensuring the controls are implemented, adhered to and reviewed as necessary.
- [10] **Divisional System Security Officer (DSSO) :** SSO from each division will be appointed as a DSSO. The DSSO carries the same responsibilities as a SSO and in addition is responsible for representing the SSO in their division at the ISMG.
- [11] **System Security Officer (SSO) :** A senior user will be appointed to fulfill the role of system security officer for each major application system or group of systems. SSO responsibilities focus on business aspects of security thus ensuring that the information security of the system meets all relevant business control objectives.
- [12] **System Owner:** System owners carry the overall responsibility for the information security of their own systems. They are responsible for allocation of protective marking to their systems and data according to the information classification policy and all staff for treating protectively marked material accordingly.
- [13] **Line Managers:** All line managers are responsible to take appropriate steps to ensure that all live or developing IT systems compliance with the aims and objectives of this policy.
- [14] **Users:** All users of live IT systems are required to comply with the security procedures for their system and any applicable general IT security guidance.

**9.9 Responsibility Allocation**

The responsibilities of management and information security should be set out in the policy and includes as follows -

- ◆ An owner Would be appointed for each information asset.
- ◆ All staff should be aware of the need for information security and their responsibilities.
- ◆ All new network communication links must be approved.
- ◆ A contact list of organizations that may be required in the event of a security incident to be maintained.
- ◆ Risk assessments for all third party access to the information assets must be carried out.
- ◆ Access by third parties to all material must be strictly limited and controlled.
- ◆ All outsourcing contract must detail all major changes to software and hardware.

**9.10 Asset classification and security classification**

- ◆ An inventory of assets must be maintained.
- ◆ A formal, documented classification scheme should be in place and all staff must comply with it.
- ◆ The originator or 'owner' of an item of information should provide a security classification.
- ◆ The handling of information, which is protectively marked CONFIDENTIAL must be specifically approved.
- ◆ Exchanges of data and software between organizations must be controlled. Organizations to whom information is to be sent must be informed of the protective marking associated with mat information.
- ◆ Appropriate procedures for information labelling and handling must be agreed and put into practice.
- ◆ Classified waste must be disposed of appropriately and securely.

**9.11 Access control**

- ◆ Access controls must be in place to prevent unauthorised access to information systems and computer applications.
- ◆ Access must only be granted in response to a business requirement. 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.



- ◆ 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 will be provided with a unique user identifier.
- ◆ It should not be permitted for an individual to use another person's user Id.
- ◆ PCs and terminals should never be left unattended whilst they are connected to applications or the network.
- ◆ Password policy should be defined and the structure of password and the duration of the password should be specified. Password must be kept confidential.
- ◆ When using mobile computing facilities such as laptops, notebooks, etc. special care should be taken to ensure that business information is not compromised, particularly used in public places.

**9.12 Incident Handling**

- Security incident reporting approach must be developed. Specific procedures must be introduced to ensure that incidents are recorded and any recurrence is analysed to identify weakness or trends.
- Procedures for the collection of evidence relating to security incident should be standardized. Adequate records must be maintained and inspections facilitated to enable the investigation of security breaches.

**9.13 Physical and Environmental Security**

- ◆ Physical security should be maintained and checks must be performed to identify all vulnerable areas.
- ◆ The IT infrastructure must be physically protected.
- ◆ Access to secure areas must remain limited to authorised staff only.
- ◆ Confidential and sensitive information and valuable assets must always be securely locked when not in use.
- ◆ Computers must never be left unattended whilst displaying confidential or sensitive information.
- ◆ Supplies and equipment must be delivered and loaded in an isolated area to prevent any unauthorised access to key facilities.
- ◆ Equipment, information or software must not be taken off-site without proper authorisation.
- ◆ 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.

**9.14 Business Continuity Management**

- ◆ A Business Continuity Plan (BCP)) must be maintained, tested and updated if necessary. All staff must be made aware of it.
- ◆ A Business Continuity and Impact Assessment must be conducted annually.
- ◆ Suppliers of network services must be contractually obliged to provide a predetermined minimum service level.

**9.15 System Development and Maintenance Controls**

- System development or enhancement must have appropriate security controls included to safeguard their availability and ensure confidentiality of the information they process.
- All security requirements and controls must be identified and agreed prior to the development of information system.

**9.16 IS Audit Policy**

**9.16.1 Purpose of the audit policy**

- Purpose of the audit policy is to provide the guidelines to the audit team to conduct an audit on IT based infrastructure system.
- The audit policy should lay out the objective and the scope of audit. An audit is conducted to -
  - ◆ Safeguard of information system assets / resources
  - ◆ Maintenance of data integrity
  - ◆ Maintenance of system effectiveness
  - ◆ Ensuring system efficiency
  - ◆ Compliance with information system related policies, guidelines and any other instructions requiring compliance in whatever name called.
- The IS audit is done to protect entire system from the most common security threats which includes the following:
  - ◆ Access to confidential data
  - ◆ Unauthorised access to the department computers.
  - ◆ Password disclosure compromise
  - ◆ Virus infections
  - ◆ Denial of service attacks.
  - ◆ Open ports, which may be accessed from outsiders
  - ◆ Unrestricted modems unnecessary open ports.

### **9.16.2 Scope of IS audit**

The scope IS auditing should encompass the examination and evaluation of the adequacy and effectiveness of the internal control and the quality of performance by the information system, to determine whether reasonable assurance exist that objectives and goals will be achieved.

The scope of audit will also include the internal control system(s) for the use and protection of -

- ◆ Data
- ◆ Technology
- ◆ People
- ◆ Application systems
- ◆ Facilities

The IS auditor will examine the followings -

- ◆ Information system mission statement and agreed goals and objectives.
- ◆ 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.
- ◆ Information system budgets and monitoring or variances.
- ◆ Policies for information system use and monitoring of compliance with these policies.
- ◆ Major contract approval and monitoring of performance of the supplier.
- ◆ Monitoring of performance against service level agreement.
- ◆ Acquisition of major systems and decisions on implementation.
- ◆ Impact of external influence on information system such as internet.
- ◆ Control of internal and external audit reports, quality assurance reports or other reports on information system.
- ◆ Business Continuity Planning, and Testing.
- ◆ Compliance with legal and regulatory requirements.

### **9.16.3 What Audit policy should do**

The audit may be conducted by internal or external auditor. IS auditor should be independent of the activities they audit. The Audit policy should essentially do the following -

- ◆ The audit policy should lay down the responsibility of audit
- ◆ The policy should lay out the periodicity of reporting and the authority to whom the reporting is to be made.
- ◆ A statement of minimum qualification & experience requirements of the auditors.
- ◆ All IS auditors will sign a declaration of fidelity and secrecy before commencing the audit work.

- ◆ The policy may lay out the extent of testing to be done, such as -
  - Planning
  - Compliance Testing
  - Substantive Testing
- ◆ A documented audit program would be developed including -
  - Documentation of the auditor's procedures for collecting, analysing interpreting information during the audit.
  - Objectives of the audit.
  - Scope, nature and degree of testing required to achieve the audit objective.
  - Identification of technical aspect, risks, processes and transactions which should be examined.
  - Procedures for audit prepared prior to the commencement of audit work.
- ◆ 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 communication device.
  - Access to information that may be produced, transmitted or stored on Depts.
  - Access to work areas.
  - Access to reports / documented created during internal audit.
  - Access to interactively monitor and log traffic on network.
- ◆ The policy should outline the compliance testing areas -
  - Organizational and operational controls
  - Security management controls
  - System development and documentation controls.
  - Application controls
  - Physical and environmental controls
  - Access controls
  - Business Continuity Controls.
- ◆ The auditor will carry out substantive testing wherever the auditor observe 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.

### **9.17 Audit Working Papers and Documentation**

All significant matters which requires the judgment, together with the auditor's conclusion should be included in the working papers. The form and contents of the working papers depends on -

- ◆ 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 with information of succeeding audit, 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 organisation structure of the entity.
- ◆ The IS policies of the organization.
- ◆ The historical background of the information system.
- ◆ Extracts of copies of important legal document relevant to audit.
- ◆ A record of the study and evaluation of the internal controls.
- ◆ Copies of audit reports and observations of earlier years.
- ◆ Copies of management letters issued by the auditor.

The current file normally includes -

- ◆ Correspondence relating to the acceptance of appointment and the scope of the work.
- ◆ Document 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 each procedures.
- ◆ Copies of letters and notes concerning audit matters communicated or discussed with the client.
- ◆ Letters of representation and confirmation received from the client.
- ◆ Conclusions reached by the auditor concerning significant aspect of the audit.
- ◆ 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.

#### 9.17.1 Planning the documentation

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

- [1] **The Understanding:** Understanding of the planning process and its importance requires identifying three planning question -
  - ◆ **Knowing your resources:** The three basic resources -time, people, money. One has to check for their availability and affordability.
  - ◆ **Defining the scope and audience:** Report may undergo significant changes depending on the character of report and nature of audience. Presentation on balance 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.
- [2] **The Documentation Writer:** The qualities and skills that the documentation writer would need. The requirement may often be legal in nature.
- [3] **Rules to guide documentation writing:** The four steps of writing documentation described in subsequent section.

#### 9.17.2 Gathering Information

It is necessary to get information about the reader and the requirement of the document.

- ◆ **About the Reader:** Task analysis can be performed to find information about the reader. Three parts of the task: 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.

#### 9.17.3 Organizing Information

Involves deciding what information to include and how to sequence it. There are four aspect of organising information -

- ◆ **Selecting Information :** Selecting what the reader needs to know and organising into a useful sequence.
- ◆ **Organising the Documentation:** Using the five organisational sequences - Subject, Difficulty, Chronological, Importance and Analytical.
- ◆ **Dividing Into Sections:** Dividing documentation into chapters into sections.
- ◆ **Dividing Into Subsections:** Dividing sections or chapters into subsections.

#### 9.17.4 Writing the Documentation

The basic principles involved are as follows -

- ◆ Writing in Active Voice:
- ◆ Giving the Consequences:
- ◆ Writing from General to Specific:
- ◆ Consistency:
- ◆ Writing Online Documentation:

#### 9.17.5 Finalizing Documents

This section identifies the tasks involved in reviewing testing, indexing and formatting the document-

- ◆ **Reviewing and Tasting:** Selection of reviewer of the documentation involves identification of subject and communication skill. In order to ensure objectivity it is recommended that reviewer be a person who has not been involved in the documentation process.
- ◆ **Generating the Glossary and Index:** In order to achieve this task it is necessary to mark the index and glossary entries at the stage of documentation itself.
- ◆ **Formatting and Production:** This involves choosing effective formatting options for headings, sub-headings, section breaks, formatting, and allied. Appropriate binding style.

#### 9.18 IS Audit Reports

Audit reports broadly include the following sections -

- ◆ **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 report's date of issue. The title page may also indicate the names of the audit team members.
- ◆ **Table of Contents :** The table lists the sections and sub-sections with page numbers including summary and recommendations.
- ◆ **Summary / Executive Summary:** The summary gives a quick overview of the salient features at the audit in. It should not normally exceed three pages, including the recommendations.
- ◆ **Introduction:** It should the following elements -

**Context:** This sub-section briefly describes the entity's role, size and organisation especially with regard to information system management, system management during the period under review, events that need to be noted, results of internal audits or.

**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.

**Methodology:** This section briefly describes sampling, data collection techniques and the basis for auditors' opinions. It also identifies any weaknesses in the methodology.

- ◆ **Findings :** The main part of an audit report. They result from the examination of each audit issue in the context of objectives and clients' expectations.
- ◆ **Opinion:** If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in consonance to the requirement.
- ◆ **Appendices :** They usually include comprehensive statistics, quotes from publications, documents, and references.

**Level of Detail:** The depth of coverage should normally reflect the significance of the findings. Situations representing a high degree of risk or indicating shortcomings to justify a recommendation should be treated extensively. Specific initiatives that the auditors wish to mention as examples should be described in detail.

**Commentary :** Where a recommendation and a compliment are made under the same issue, they should be in separate paragraphs, otherwise, they may confuse the reader. Statistics need to be used consistently through out the report. The size of the population, the number of transactions and the period of time provide that context.



**PRIME VISION / C.A. FINAL / ISCA / DRAFTING OF IS SECURITY POLICY, AUDIT POLICY, IS AUDIT REPORTING & PRACTICAL PERSPECTIVE**

|                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>WHAT INFORMATION IS SENSITIVE:</b></p> <ul style="list-style-type: none"> <li>• Strategic Plans</li> <li>• Business Operations</li> <li>• Finances</li> </ul>                                                                                                                                            | <p><b>WHAT STEPS ARE NEEDED TO TAKE TO KEEP CRITICAL INFORMATION PROTECTED:</b></p> <ul style="list-style-type: none"> <li>• Not all data has the same value</li> <li>• Know where the critical data resides</li> <li>• Develop an access control methodology</li> <li>• Protect information stored on media</li> <li>• Review hardcopy output</li> </ul>      | <p><b>PROTECTING COMPUTER-HELD INFORMATION SYSTEMS:</b></p> <ul style="list-style-type: none"> <li>• Need to know what the information systems are and where these are located.</li> <li>• Need know the value of the information held and how difficult it would be to recreate if it were damaged or lost.</li> <li>• Need to know who is authorised to access the information and what they are permitted to do with the information.</li> <li>• Need to know how quickly information needs to be made available should it become unavailable for whatever reason</li> </ul> |
| <p><b>TYPES OF PROTECTION THAT AN ORGANISATION CAN USE:</b></p> <p>4. Preventative Information Protection</p> <ul style="list-style-type: none"> <li>• Physical</li> <li>• Logical (Technical)</li> <li>• Administrative</li> </ul> <p>5. Restorative Information Protection</p> <p>6. Holistic Protection</p> | <p><b>INFORMATION SECURITY POLICY: A</b></p> <p>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 organisation.</p> | <p><b>ISSUES TO ADDRESS:</b></p> <ul style="list-style-type: none"> <li>• A definition of information security</li> <li>• Reasons why information security is important to the organisation, and its goals and principles</li> <li>• A brief explanation of the security policies, principles, standards and compliance requirements</li> <li>• Definition of all relevant information security responsibilities</li> <li>• Reference to supporting documentation</li> </ul>                                                                                                    |

**PRIME VISION / C.A. FINAL / ISCA / DRAFTING OF IS SECURITY POLICY, AUDIT POLICY, IS AUDIT REPORTING & PRACTICAL PERSPECTIVE**

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>TYPES OF INFORMATION SECURITY POLICIES AND THEIR HIERARCHY: (<u>U</u> <u>A</u> <u>n</u> <u>d</u> <u>I</u> <u>C</u> <u>a</u> <u>n</u> <u>O</u> <u>b</u> <u>v</u> <u>i</u> <u>s</u> <u>o</u> <u>b</u> <u>l</u> <u>i</u> <u>n</u> <u>e</u> <u>s</u> <u>s</u> <u>l</u> <u>y</u> <u>N</u> <u>a</u> <u>i</u> <u>l</u> <u>i</u> <u>t</u>)</b></p> <ul style="list-style-type: none"> <li>• <u>U</u>ser Security Policy</li> <li>• <u>A</u>ceptable Usage Policy</li> <li>• <u>I</u>nformation Security Policy</li> <li>• <u>C</u>onditions of Connection</li> <li>• <u>O</u>rganisational Information Security Policy</li> <li>• <u>N</u>etwork &amp; System Security Policy</li> <li>• <u>I</u>nformation Classification Policy</li> </ul> | <p><b>COMPONENTS OF THE SECURITY POLICY:</b></p> <ul style="list-style-type: none"> <li>• Purpose and Scope of the Document and the intended audience</li> <li>• The Security Infrastructure</li> <li>• Security policy document maintenance and compliance requirements</li> <li>• Incident response mechanism and incident reporting</li> <li>• Security organisation structure</li> <li>• Inventory and Classification of assets</li> <li>• Description of technologies and computing structure</li> <li>• Physical and Environmental Security</li> <li>• Identify Management and access control</li> <li>• IT Operations management</li> <li>• IT Communications</li> <li>• System Development and Maintenance Controls</li> <li>• Business Continuity Planning</li> <li>• Legal Compliances</li> <li>• Monitoring and Auditing Requirements</li> <li>• Underlying Technical Policy</li> </ul> | <p><b>PURPOSE OF THE AUDIT POLICY:</b><br/>To provide the guidelines to the audit team to conduct an audit on IT based infrastructure system. Common security threats are:</p> <ul style="list-style-type: none"> <li>• Access to confidential data</li> <li>• Unauthorised access of the computers</li> <li>• Password disclosure compromise</li> <li>• Virus infections</li> <li>• Open ports, which may be accessed from outsiders</li> <li>• Unrestricted modems unnecessarily open ports</li> </ul> <p><b><u>Objective and the scope of the IS Audit policy:</u></b></p> <ul style="list-style-type: none"> <li>• Safeguarding of Information System Assets/Resources</li> <li>• Maintenance of Data Integrity</li> <li>• Maintenance of System Effectiveness</li> <li>• Ensuring System Efficiency</li> <li>• Compliance with Information System related policies, guidelines, circulars, and any other instructions requiring compliance in whatever name called.</li> </ul> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**PRIME VISION / C.A. FINAL / ISCA / DRAFTING OF IS SECURITY POLICY, AUDIT POLICY, IS AUDIT REPORTING & PRACTICAL PERSPECTIVE**

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>SCOPE OF IS AUDIT:</b> 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:</p> <p><b>(Did Tendulkar Pay A Fine)</b></p> <ul style="list-style-type: none"> <li>• <u>D</u>ata</li> <li>• <u>T</u>echnology</li> <li>• <u>P</u>eople</li> <li>• <u>A</u>pplication systems</li> <li>• <u>F</u>acilities</li> </ul> | <p><b>AUDIT WORKING PAPERS AND DOCUMENTATION:</b></p> <ul style="list-style-type: none"> <li>• The nature of the engagement</li> <li>• The form of the auditor's report</li> <li>• The nature and complexity of client's business</li> <li>• The nature and condition of client's records and degree of reliance on internal controls</li> <li>• The permanent audit file</li> <li>• The current file</li> </ul> | <p><b>IS AUDIT REPORTS:</b><br/><b>(Can Tina Sit Front Of Anil?)</b></p> <ol style="list-style-type: none"> <li>1. <u>C</u>overed and Title Page</li> <li>2. <u>T</u>able of Contents</li> <li>3. <u>S</u>ummary/Executive Summary</li> <li>4. <u>I</u>ntroduction <ul style="list-style-type: none"> <li>• Context</li> <li>• Purpose</li> <li>• Scope</li> <li>• Methodology</li> </ul> </li> <li>5. <u>F</u>indings</li> <li>6. <u>O</u>pinion</li> <li>7. <u>A</u>ppendices</li> </ol> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---\*\*\*\*---