CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION:

The purpose of Information Security is to protect the valuable resources of an organization such as hardware, software and skilled people. Through the selection and application of appropriate safeguard, security helps the organization to meet its business objectives or mission by protecting its physical and financial resources, reputation, legal position, employees and other tangible and intangible assets.

Information systems security begins and ends with the people within the organization and with the people that interact with the system, intentionally or otherwise. The end-users who try to access the information which the security professionals are trying to protect could be the weakest link in security chain. By understanding some of the behavioral aspects of organizational science and change management, security administrators can greatly reduce the levels of risk caused by end users and create more acceptable and supportable security profiles. These measures, along with appropriate policy and training can substantially improve the performance of end users and result in a more secured information system.

This Researcher has collected comprehensive information from various books, manuals, magazines, journals, articles and research websites. Information gathered through various seminars and conferences attended by her also helped lot for the researcher.

2.2 ELEMENTS OF INFORMATION SECURITY:

Thomas R. Peltier who is an Information security professional since 1977, has provided guidelines for effective Information Security Management. Referring to his guidelines\(^1\), information security should be based on following eight major elements

a. Information protection should support objectives of business or mission of enterprise.

Many times information security personnel lose track of their goals and responsibilities. The post of Information Security Officer has to be created to support enterprise security.
b. Information protection is an integral element for necessary care. Senior management is endowed with two basic responsibilities such as duty of loyalty and duty of care. A duty of loyalty implies that the decisions shall be made in the best interest of the enterprise and duty of care implies that senior management shall protect the assets of the enterprise and make informed business decisions.

c. Information protection must be cost-effective. Implementation of controls must be proposed and it is necessary to confirm that a significant risk exists. Implementing a timely risk analysis process can accomplish this.

d. Information security responsibilities and accountabilities should be made explicit. For any program to be more effective, it is necessary to publish information security policy statement and information security group mission statement. The information security policy should identify roles and responsibilities of all employees. To make the policy more effective the language of the policy must be incorporated into purchase agreements for all contract personnel and consultants.

e. Systems owners have information protection responsibilities within the own organization. Access to information often extends beyond the organization also. This is the responsibility of information owner. The main responsibility is to monitor the usage to ensure that it complies with the user profile and authorization of the users. If system has external users then the owners have the responsibility to share appropriate level of knowledge about the existence and general extent of control measures so that other users can be confident that the system is adequately secured.

f. Information protection requires a comprehensive and integrated approach. For its effectiveness, it is necessary that the information security and its protection shall be a part of the system development lifecycle. During initial or analysis phase, information security should include risk analysis, a business impact analysis and information classification document. Additionally, because information is resident in all departments throughout the enterprise, each business unit should establish an individual responsible for implementing the information protection program to meet the specific business goals of the department.

g. Information security should be periodically reassessed with respect to time, need and objectives. A good information protection program examines itself on a regular basis and makes changes wherever and whenever necessary. This should be a dynamic
Chapter 2: Literature Review

process hence must be reassessed every eighteen months or even earlier on extraordinary occasions.

h. Information protection is constrained by culture of the organization. The information System Security Officer must understand and advice basic information security program that must be implemented throughout the enterprise. However, each business unit should be given latitude to make modifications to meet its specific needs. For a multinational company, it is necessary to make region or culture based adjustments for each of various countries.

2.3 SECURITY PRINCIPLES:
Following are some of the guidelines issued by Economic Cooperation and Development intended for development of laws and policies:

a. Accountability: Everybody involved with the security of information must have specified accountability towards actions.

b. Awareness: Everyone from the organization must be able to access the knowledge pertaining to security measures, practices and procedures and all efforts shall be made in building confidence in information systems.

c. Ethics: The method in which information systems and their associated security mechanisms are operated must be able to respect the privacy, rights and legitimate interests of users.

d. Multidisciplinary principle: All the aspects and opinion must be considered in the development of policies, procedures and techniques. These must include legal, technical, administrative, organizational, operational, commercial and educational aspects.

e. Proportionality: Security measures must be based on the value of information and the level of risk involved.

f. Integration: Security measures must be integrated to work together and establish defensive depth in the security system.

g. Timeliness: Everyone should act together in coordinated and timely fashion when a security breach occurs.

h. Reassessment: Security mechanisms and needs must be reassessed periodically to ensure that organizations needs are being met.
i. **Democracy**: The security of the information and the systems where it is stored must be in line with the legitimate use and information transfer of that information. In addition to these security principles, some additional principles are important when defining policies. These include:

j. **Individual accountability**: Individuals are uniquely identified to the security systems and users are held accountable for their actions.

k. **Authorization**: The security mechanisms must be able to grant authorization for access to specific information or systems based on the identification and authorization of the user.

l. **Least privilege**: Individuals must be able to access the information that they need for the completion of their related task or job responsibilities, and only for as long as they do that job or complete respective task.

m. **Separation of Duty**: Functions must be divided between people to ensure that no single person can commit a fraud, which can go undetected.

n. **Auditing**: The work being done, the associated results must be monitored to ensure compliance with established procedures and the correctness of the work being performed.

### 2.4 INFORMATION SECURITY POLICIES, STANDARDS AND PRACTICES:

Before examining various types of information security policies, it is important to understand the relation between policies, standards and practices. As per the Director of Policies and Administration for the Netigy Corporations, Global security practice, Policies, standards and procedures fit into following hierarchy.

1. A policy states a goal in general terms.
2. Standards define what is to be accomplished in specific terms.
3. Procedures tell how to meet the standards.

Following example illustrates the hierarchy of policies, standards and procedures.

#### 2.4.1 Policies:

It is a high level statement for a company or enterprise beliefs, goals and objectives and general means for their attainment for a specified subject area. Policy Content Consideration: A policy document should be approved by Management, published and communicated, as appropriate to the employees. It
Chapter 2: Literature Review

should state management commitment and set out organization’s approach to managing information security.

Following contents should be included in a Policy\textsuperscript{[2]}:

a. A definition of information security, its overall objectives, scope and importance of security as an enabling mechanism for information sharing.
b. A statement of management intention, supporting the goals and principles of information security.
c. A brief explanation of specific security policies, standards and compliance requirements including compliance with legislative and contractual requirements as well as security awareness and education requirements.
d. Satisfy legal and contractual requirements for security.
e. Provide enforcement and recovery guideline (including insurance coverage) for instances when a compromise of security is detected.
f. Protect and provide a secure and safe work environment for its employees.

\begin{figure}
\centering
\includegraphics[width=\textwidth]{Figure2_1}
\caption{Figure: 2.1: Policies, Standards and Practices source: CRC Press, Information Security policies, procedures and Standards}
\end{figure}

From the above figure policy is a plan of action to convey instructions issued by senior management to its concern staff which performs duties on the behalf of
organization while standards are the detailed statements which specify what must be
done to comply the policy whereas Practices, Procedures and Guidelines effectively
explains how to implement the policy.

2.4.2 Information security Policy Infrastructure:

Information security policy is composition of following elements:

a. **IT Asset Inventory:** This includes all IT assets of organization such as hardware and
   software resources because; basic objective of information security is to protect the
   assets of organization.

b. **Known attacks:** These are mainly viruses, insiders, hackers and crackers which are
   usually stealing the information.

c. **Data classification:** This is an important facet of the policy and it is a control for
   protection of data. It is used to differentiate the data as general and confidential one.
   For confidential data company policy classified them as “for internal use only”.

d. **Procedures:** Procedures spell out the specifics of how the policy and the supporting
   standards and guidelines will actually be implemented in an operating environment.

e. **Team:** This is a group of people together who are actually involved in managing the
   security.
f. **Compliance**: It states that who is responsible for ensuring the security of specific domain and what happens when policy is violated.

g. **Feedback mechanism**: This mechanism works usually after implementation of a security policy. This mechanism is used to update the policy with some changes or modifications in the existing policy suggested by people who are implementing the policy.

h. **Best Practices**: This is generally the methodology used for implementation of the policy.

i. **IT Security organization**: This is information security organization structure which represents hierarchy of security professionals based on their profile in the organization.

j. **Management Support**: Top Management plays a major role in decision making and these decisions are strategies which are further communicated as policies.

### 2.4.3 Policy Design Life Cycle:

![Policy Design Life Cycle Diagram](image)

**Figure 2.3: Policy Design Life Cycle**

Entire Policy design life cycle is made up of total eight phases such as given below:
Chapter 2: Literature Review

a. **Asset Inventory**: An asset is organizational resource that is being protected. Asset can be logical such as web site, information or data or asset could be physical like a person, computer system or other tangible object. Particularly, information assets are the focus of security efforts and are what is being protected. This is why inventory of assets is needed to identify the risk associated with related assets.

b. **Risk Analysis**: In information security, risk could be the probability of a threat to the system, the probability of vulnerability being discovered or probability of equipment or software malfunctions. Risk analysis can be the risk which can be measured in terms of qualitative or quantitative terms.

c. **Policy**: Once the risk is identified, organization objective is to protect those assets so as to reduce the risk. Policy is high level statement of organization for attainment towards protection of information assets of organization.

d. **Procedure**: As discussed earlier, procedures are focused on how the policy will be actually implemented in operating environment.

e. **Implementation**: This is actual execution of a policy based on certain standards and guidelines followed by the organizations.

f. **Training**: This involves providing awareness to the members of the organization with detailed information and hands-on instruction to prepare them to perform their duties securely.

g. **Feedback**: After implementation is in process, the opinions of the users are taken about the procedures and standards applicable to the policy. With appropriate opinions the policy can be further modified or updated.

h. **Update**: This is the last phase of the policy design life cycle where changes in the existing policy are reviewed and implemented in the specific policy.

2.4.4. Policy design process:

a. **Business Objective**: Policies are written to support mission, vision and strategic planning of organization. The mission of an organization is a written statement of organization that supports business objectives while vision statement of an organization is a written statement of organization that supports goals of organization.

b. **IT Plan**: This is a planning for procurement of hardware and software as per the requirements of current and future technologies in the organization. It is also focused on the projects which are in pipeline.
c. **Existing Procedures**: Procedures specifies how specific guidelines and standards are actually implemented in an operating environment. Procedures are either technology or process dependant and refer to specific platforms, applications and processes.

d. **Risk Management**: This is the process of identifying vulnerabilities in the organization’s information systems and taking carefully reasoned steps to ensure confidentiality, Integrity and availability of all the components in the information systems.

e. **Best Practices**: These are the methodologies or processes adopted by organization in order to ensure that security measures have been correctly handled.

f. **Possible Threats**: In the context of Information security, a threat is an object, person, or other entity that represents a constant danger to assets of organization. Possible threats could be unauthorized access or stealing of information or disclosure of information.

g. **IT Assets Inventory**: Basic objective of information security is to safeguard assets of organization. IT assets are hardware components, supporting software and skilled people working in the organization.
2.4.5 Structure of Documented Policy:

The structure of the policies documented may be as follows:

1.0 Overview
   <Brief background and need for the formulation of Policy>

2.0 Purpose
   <Purpose of the Policy. Brief explanation about the security hazards in absence of this policy>

3.0 Scope
   <Detail description of the scope of the policy, i.e. where it is applicable, who should follow, who will be affected and who shall be responsible. Generally all security policies are applicable to entire organization>

4.0 Policy
   <Detail Policy Statements with proper numbering mechanism so as to trace the same to the procedures. There could be more than one policy statement under each section. The format of Policy statement can be>
   <Section Number>.<Policy Number> <Policy Statement>
   <Section Number>.<Policy Number> <Policy Statement>

4.1 Guidelines
   <Include guidelines on how to implement the policy. Procedure to follow the policies. IT Processes that gets affected by the policies>

5.0 Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
   <Also other procedures may be included here>

6.0 Definitions
   <Give the detail descriptions of the terms used in the policy statements>

Terms Definitions

7.0 Revision History
   <All details about the revisions made in the policy statements>
   Subsequent implementation should be documented here>

[Source: CSI Bangalore]
2.4.6. Administrative Policies vs. Technical Policies

Technical security policies describe how technology should be configured and used, and administrative security policies describe how people (end-users and management) should behave. The intended security rules for technology systems and data should be explicitly described in technical security policies. Technical security policies describe a rule or regulation pertaining to a piece of equipment, facility, or data.

Administrative security policies describe the intended behavior rules for people. Serving as a guide for both end-users and management, administrative policies should spell out the roles and responsibilities for all users of technology systems in the organization. It is very important to inform end-users and other management team members of administrative security policies. Users cannot be expected to follow policies if they do not know what they are. After reviewing the administrative policies, it is a good idea to get the user to sign the policy document attesting to the fact that they have read it, understand it and will abide by it.

Many organizations take the time to define technical security policies, while administrative security policies are often overlooked. While many technical security policies can be audited with online scanning tools, administrative security policies can only be audited with an in-person review. Auditors who review administrative policies will typically ask to see the actual formal policy document. Efficient auditors will also interview end-users and management to see if they understand their roles and responsibilities.

2.4.7 Security Standards:
The BS 7799 / ISO 17799 Standard is written and published in two parts[^3]:

1) ISO/IEC 17799 Part 1:
Code of practice for information security management is a guide containing advice and recommendations to ensure the security of a company’s information according to ten fields of application.
2) **BS 7799 Part 2:**

Information security management -- specifications with guidance for use provides recommendations for establishing an effective Information Security Management System (ISMS). At audit time, this document serves as the assessment guide for certification. BS7799 provides conditions for information security management. Comprised the ten domains and 127 controls of the ISO 17799 standard, this reference applies to the development, implementation and maintenance stages of an information security management system. Organizations applying for certification are evaluated according to this document. An organization that bases its ISMS on the provisions in BS 7799 can obtain certification from an accredited body. The organization thereby demonstrates to its partners that its system both complies with the standard and answers the need for security measures as determined by its own requirements.

### 2.4.7.1. History of the BS7799 / ISO 17799 standard:

For over a hundred years, the British Standards Institution (BSI) has carried out studies for the purpose of establishing effective, high-quality industry standards. BS 7799 was developed at the beginning of the 1990s in response to industry, government and business requests for the creation of a common information security structure. In 1995, the BS7799 standard was officially adopted.

Four years relapsed before the publication in May 1999 of a second major version of the BS 7799 standard, incorporating numerous improvements. It was during this period that the International Organization for Standardization (ISO) began to take an interest in the work published by the British institute.

In December 2000, ISO took over the first part of BS 7799, re-baptizing it ISO 17799. In September 2002, a revision of the second part of the BS7799 standard was carried out in order to make it consistent with other management standards such as ISO 9001:2000 and ISO 14001:1996 as well as with the principles of the Organization for Economic Cooperation and Development (OECD). Currently, consultations are taking place at the international level to keep BS 7799 / ISO 17799 at the leading edge of the latest developments.
The international standard ISO/IEC 17799 was developed by the British Standards Institution (BSI) as BS 7799. It was adopted through a special “fast track procedure” by the JTC 1 (Joint ISO/IEC Technical Committee), concurrently with its approval by the national member institutes of ISO and the IEC. ISO/IEC 17799 is presented in the form of guidelines and commendations that were assembled following consultations with big business. The 36 security objectives and 127 security controls contained in ISO/IEC 17799 is divided among ten domains. The following is a brief overview of each of these domains:

a. **Security Policy** - Provide guidelines and management advice for improving information security.

b. **Organizational Security** – Facilitate information security management within the organization.

c. **Asset Classification and Control** – Carry out an inventory of assets and protect these assets effective.

d. **Personnel Security** - Minimize the risks of human error, theft, fraud or the abuse of equipment.

e. **Physical and Environmental Security** - Prevent the violation, deterioration or disruption of industrial facilities and data.

f. **Communications and Operations Management** - Ensure the adequate and reliable Operation of information processing devices.

g. **Access Control** - Control access to information

h. **Systems Development and Maintenance** - Ensure that security is incorporated into information system.

i. **Business Continuity Management** – Minimize the impact of business interruptions and protect the company’s essential processes from failure and major disasters.

j. **Compliance** - Avoid any breach of criminal or civil law, of statutory or contractual requirements, and of security requirements.

### 2.4.7.2 What is PDCA Model?

In this field of information technology, it is essential to integrate multiple initiatives within a corporate strategy so that each element provides an optimal level of
protection. This is where information security management systems come into play – they ensure that all efforts are coordinated in order to achieve optimum security. A management system must therefore include an evaluation method, safeguards and a documentation and revision process. This is the underlying principle of the PDCA (Plan-Do-Check-Act) model which strongly resembles the ISO 9001 model for quality management. [5]

Figure 2.5: PDCA Model
Source: (BS 7799: Major process Steps)-Courtesy of Gamma Security System
Plan
- Define the ISMS scope and the organizations security policies
- Identify and assess risks
- Select control objectives and controls that will help to manage these risks.
- Prepare the statement of applicability

Do
- Formulate and implement a risk mitigation plan
- Implement the previously selected controls in order to meet the control objectives.

Check
- Perform monitoring procedures
- Conduct periodic reviews to verify the effectiveness of the ISMS
- Review the levels of acceptable and residual risk
- Periodically conduct internal ISMS audits

Act
- Implement identified ISMS improvements
- Take appropriate corrective and preventive action
- Maintain communications with all stakeholders
- Validate improvements.

2.4.7.3 BS 7799 To 27001:
BH consulting have published one paper in May 2006 on the topic `BS 7799 TO Become 27001`. This paper indicates that BS 7799 is divided into two parts. The first part is intended for setting of best practices for Information Security. This part is split up into ten sections which cover following areas.

- Security Policy
- Security Organization
- Physical and Environmental
- Asset classification
- Personnel security
Chapter 2: Literature Review

- Access control
- System development and maintenance
- Communication and operations management
- Business continuity planning
- Compliance.

Second part of BS 7799, outlined the 127 controls, which an organization can implement to achieve the standard. It is against part two of standard; the company can be independently audited and subsequently certified. There are many similarities in BS7799 and ISO 27001; this BS 7799 will be replaced by ISO 27001 at the end of 2005.

ISO 27001 is more closely aligned with ISO 17799 as it is based on PDCA model.

![Trends in the Global Uptake of BS 7799](chart21.png)

**Source:** International ISMS/BS 7799 Certification Newsletter, July 2003

**Chart 2.1: Trends in Global Uptake of BS 7799**

### 2.4.7.4 Background and purpose of ISO 27001:

Information shield published one white paper on IEC/ISO 270001 Certification [6]. According to this paper, before the international information security standard known as ISO 17799, there was the preceding British Standard BS7799, published by the British Standards Institute (BSI). The original BS 7799 had two parts. BS 7799 Part1 -
Chapter 2: Literature Review

*Code of practice for information security management* - established the overall requirements for an information security program by breaking security into ten separate topic domains.

BS 7799-1 was eventually adopted as the first international standard for information security [7]. ISO 17799:2000 [1]. BS 7799 Part 2, entitled *Information security management systems — Specification with guidance for use*, was designed to allow an organization to become certified that it was following the techniques defined in Part 1 of the standard.

Within Great Britain and around Europe, hundreds of organizations became certified against BS7799. Up until last year, if an organization wished to become “certified”, it could only be done against the British Standard BS7799.

In 2005, the International Organization for Standardization (ISO) took two important steps relating to information security. First, it updated ISO 17799:2000 and called it ISO 17799:2005 (See the related Information Shield whitepaper, “What’s new with the ISO 7799:2005 – Policy Implications for Business.”). Second, it adopted the part 2 of BS 7799 and released it as *ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements*. For the first time, organizations can get certified against the ISO 17799:2005 standard.

By definition, ISO 17799:2005 and ISO 27001 are designed to be used by any organization in any industry. However, many smaller organizations may have trouble meeting some of the requirements of ISMS due to limited manpower and resources.

**2.4.7.5 Overview of ISO 27001**

Basically, ISO 27001 sets out the requirements for how an organization can implement the security requirements of ISO 17799:2005. According to ISO 27001 [8]:

“This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).”

According to the Standard, ISM is defined as:
“The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.”

In other words, the ISMS encompass your entire information security program, including its relation to other parts of the organization. While ISO 27001 does not provide a complete prescription for a proper information security program, it does list the various organizational functions required for certification, including a list of required documents that must be produced, ISO 27001 uses a process-based approach, copying the model first defined by the organization for Economic Cooperation and Development (OECD). The Plan-Do-Check-Act (PDCA) \[^9\] breaks overall organizational processes into four phases as described earlier.

### 2.4.7.6 The Role of Information Security Policies\[^{10}\] in ISO 27001:

Written information security policies are the foundation for any Information Security Management System, and are specifically required in ISO 27001. Not only are written policies listed in the definition of an ISMS, they are referred to throughout the ISO 27001 standard. For example, part of the required documentation is an overall policy.

Defining the information security management system: The ISMS documentation shall include: documented statements of the ISMS policy and objectives; the purpose of ISO 27001 is to certify that an organization is compliant with ISO 17799:2005. The first information security domain listed in the ISO 17799:2005 standard is called “5.0 Information Security Policy.”

In fact, a written set of information security policies is often considered the best evidence of management’s support for the information security function. According to ISO 27001:

Management shall provide evidence of its commitment to the ISMS by establishing an ISMS policy.

### 2.4.7.7 Policy coverage for all ISO 17799:2005 security domains:

Information Security Policies Made Easy (ISPME) has pre-written policies \[^{11}\] for every domain and category of the ISO 17799:2005 standard, including such topics as
access controls, network security, data integrity, organizational security, personnel security, encryption, physical security, disaster recovery, incident response and many others. In fact, ISPME is organized around the ISO 17799 outline to make it easier to locate and refer policies, and to help fill in any policy gaps discovered by the organization.

2.4.7.8 Documentation requirements of ISO 27001
ISO 27001 is very clear about the documentation requirements of any information security program. In addition to over 1300 policies within the policy library, ISPME comes with fifteen separate, pre-written information security policy documents. Organizations seeking certification can save considerable time and effort by using the pre-written documents that have been used in thousands of organizations around the world\cite{12}.

In addition to policies, organizations must also document the roles and responsibilities of individuals who will perform the various functions. For example, Internal ISMS Audits: The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records shall be defined in a documented procedure.

Information Security Roles and Responsibilities Made Easy (ISRR) provide documented information security job requirements for over 40 organizational roles. In addition, ISRR provides security-related mission statements for various organizational units, and nine different information security reporting relationships and organizational diagrams. In short, ISRR is the most effective way for organizations to clearly document the security responsibilities of the entire organization as required by ISO 27001.

2.5. SUPPORTING A RISK-BASED APPROACH TO SECURITY:
ISO 27001 clearly specifies that organizations must adopt a risk-based approach to security\cite{13}. This means that organization must adopt a documented risk assessment approach, which includes a process for risk acceptance. ISPME provides over 20 prewritten policies that support the performance of risk assessments within the organization.
In addition, each of the 1300+ policies found within the ISO policy library contain expert commentary from Charles Cresson Wood, CISSP, CISM, CISA who has over 20 years of information security experience. The commentary for each policy discusses the Organizational risks that are mitigated by each corresponding policy statement.

The organization shall do the following:
Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks.

2.5.1. Management Support of Information Security:
Section 5 of ISO 27001 details the requirements for demonstrated management support of the information security function.
“Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISM”
ISPME provides information security policies that define the responsibilities of executive and senior management within the security function. For example, policies that require the establishment of executive level information security review boards and periodic management review of the information security program. In addition, ISPME provides policies that define the requirements of other critical organization roles such as data custodian, data owner, internal audit and many others. Information Security Roles and Responsibilities Made Easy (ISRR) provide over 80 prewritten documents that support an organization’s commitment to information security.
ISRR provides the “glue” that links the security requirements defined in the policies to the organizations roles responsible for performing these functions.

2.5.2. Training and awareness of Information Security:
Section 5.2.2 of ISO 27001, specifies the requirements for education and training of personnel responsible for information security. The organization shall also ensure that all relevant personnel are aware of the Relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.
Management is responsible for communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement; ISPME provides policies that specify the performance and ongoing management of Information security awareness and training. ISPME also contains a number of training and awareness methods that have proven useful in organizations worldwide. ISRR provides pre-written job descriptions for organization roles that must be involved in the training and awareness functions.

2.5.3. Monitoring and Review:
A critical component of certification with ISO 27001 is the continual monitoring and review of the information security management system. 

*Management shall review the organization’s ISMS at planned intervals (at least once a year) to ensure its continuing suitability, adequacy and effectiveness.*

Within the context of ISMS, auditing occurs at both management and technical levels. For example, information systems must be monitored for possible information security events and to preserve transaction and account integrity. Information systems must be monitored for configuration against organizational levels. At the macro level, the entire information security program should be monitored against the stated objectives of the program, and this data should be used to feed back into updates of the entire program.

*The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records shall be defined in a documented procedure.*

ISPME has specific policies for the logging and auditing of information technology and security functions, as well as high-level policies defining the business requirements for internal and external audit of the information security program.

2.5.4. Continuous Improvement
In short, ISO 27001 specifies a process of continual information security improvement through monitoring, review and action.

*The organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, information security objectives, audit results,*
ISPME helps organizations stay up to date on the latest information security technologies and threats. Now in its tenth version, ISPME has been continuously updated since its first release over 15 years ago. ISRR provides a number of resources to help information security departments secure the support and resources they need. ISRR is the only publication that allows an organization to quickly document the information security requirements of various organizational roles and departments, turning policies and procedures into real action items that are targeted at specific individuals within the organization.

### 2.6 POLICY REPRESENTATION BASED ON DOMAINS:

The representation of some of the policies such as User access Policy, Data access Policy and Physical access Policy is given below.

#### 2.6.1 User (Personnel) access policy:

**Objective:** Policies, standards and procedures must be established to address the adequate screening of potential candidates for employment. Additional controls must be implemented for those individuals working in areas with access to sensitive or competitive advantage information.

**Policy:** Individuals with access to Company information assets are expected to protect those assets. Security responsibilities are addressed during employee recruitment and activities are monitored throughout employment.

**Provisions:** Potential employees are to be adequately screened, especially for sensitive jobs. All employees and third party users of company information are subject to the contents of this policy.

**Key Terms:** Confidentiality agreements; terms and conditions of employment; security incidents; disciplinary process.

**Responsibilities:**

1. Senior management and the officers of the company are required to employ internal controls designed to safeguard company assets, including business information.
Chapter 2: Literature Review

2. It is a management obligation to ensure that all employees have clear and concise job descriptions and that all qualifications are properly verified.

3. Employees and third-party users of company information are required to read and sign a confidentiality Agreement.

Compliance:
1. Company management has the responsibility to document conditions required to obtain and maintain employment, as well as the right to monitor personnel activities.
2. Employees who fail to comply with the terms of the Confidentiality Agreement or who falsified resume information are subject to appropriate disciplinary actions.

2.6.2: Data access Policy[^16]:

Objective: Business requirements for access control must be implemented through access control rules and rights for each user or group of users must be clearly stated.

Included in this section is a determination on establishing access rules based on the policy of "access must be generally forbidden unless expressly permitted" rather than the weaker rule that "information assets are generally open unless expressly closed"

Policy: Access to all company information assets must be business-or-mission related purpose only.

Provision: Access control rules and rights for owner of the information asset must establish each individual user or group of users.

Key terms: Separation of duties, rotation of assignments, operator log, malicious software, disposal of media, information interchange.

Responsibilities:
1. Management Steering Committee is responsible for publishing access criteria.
2. Information owners are responsible for approving business-related access to information assets under their control.
3. Individuals granted access must use the information asset in accordance with owner's specifications.
Compliance:
1. Individual who exceed or attempt to exceed approved authority are subject to having access revoked.
2. Repeat violations of this policy can lead to disciplinary actions as described in employee standards of conduct.

2.6.3 Physical security policy\textsuperscript{[17]}:

Objective: It is a management responsibility to establish a safe and secure working environment. Access to company/enterprise locations must be restricted to those persons with a business need. Levels of protection must be commensurate with the value of asset and vulnerability to identified risks.

Policy: It is responsibility of company management to provide secure workplace for all the employees.

 Provision:
1. Company offices will be protected from unauthorized access.
2. Areas within buildings, which house sensitive or high risk equipment will be protected against fire, water and other hazards.
3. Devices that are critical to the operation of company business processes will be protected against power failure.

Key Terms: Security perimeter, entry controls, cabling security, secure disposal of equipment

Responsibilities:
1. Senior management and the officers of the company are required to maintain accurate records and to employ internal controls designed to safeguard company assets and property against unauthorized use or disposition.
2. The assets of Company include but are not limited to physical property, intellectual property, patents, trade secrets, copyrights, and trademarks.
Chapter 2: Literature Review

3. Additionally, it is the responsibility of line management to ensure that staff is aware of and fully complies with, company security guidelines and all relevant laws and regulations.

**Compliance**

1. Management is responsible for conducting periodic reviews and audits to ensure the compliance of all policies, procedures, practices, standards and guidelines.

2. Employees who fail to comply with the policies will be treated as being in violation of the employee standards of conduct and will be subject to appropriate corrective action.
2.7 References:


