

8. Information Systems Auditing Standards, Guidelines, Best Practices

ISO 27001 – Information Security Management Standard (ISMS)

ISO 27001 is the international best practice and standard for an information security management system. An ISMS is a systematic approach to managing confident or sensitive information so that it remains secure. It encompasses people, process and IT systems.

ISO 27001 defines how to organize information security in any kind of organization, profit or non-profit, private or state-owned, small or large. It is safe to say that this standard is the foundation of information system management.

There are mainly four phases include in the ISMS are as follows

- i. **The plan Phase** – this phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls. Detail work in this phase are as follows:
 - a. Detering the scope of ISMS;
 - b. Writing an ISMS policy;
 - c. Identifying the methodology for risk assessment and determining the criteria for risk acceptance;
 - d. Identification of assets, vulnerabilities and threats;
 - e. Evaluating the Size of risks;
 - f. Identification and assessment of risk treatment options;
 - g. Selection of controls risk treatment;
 - h. Obtaining management approval for residual risk;
 - i. Obtaining management approval for implementation of the ISMS; and
 - j. Writing a statement of applicability that lists all applicable controls, states which of them have already been implemented, and those which are not applicable.
- ii. **The do Phase** – this phase includes carrying out everything that was planned during the previous year. Detail work in this phase are as follows
 - a. Writing a risk treatment plan – describes who, how, when and with what budget applicable control should be implemented;
 - b. Implementing the risk treatment plan;
 - c. Implementing applicable security controls;
 - d. Determining how to measure the effectiveness of control;
 - e. Carrying out awareness programs and training of employees;
 - f. Management of the normal operation of the ISMS;
 - g. Implementation of procedures for detecting and manage in security incidents.
- iii. **The check phase** – the purpose of this phase is to monitor the functioning of the ISMS through various 'Channels'. And check whether the results meet the set objectives. The detail work in this phase are as follows:
 - a. Implementation of procedures and other controls for monitoring and reviewing In order to establish any violation, incorrect data processing, whether the security activities are carries out as expected etc.
 - b. Regular reviews of the effectiveness of the ISMS;
 - c. Measuring the effectiveness of control;
 - d. Reviewing risk assessment at regular intervals;
 - e. Internal audits at planned intervals;
 - f. Management reviews to ensure that the ISMS is functioning and to identify opportunities for improvement.
 - g. Updating security plans in order to take account of other montoring and reviewing activities; and

- h. Keeping records of activities and incidents that may affect the effectiveness of ISMS.
- iv. The Act phase** – the purpose of this phase is to improve everything that was identified as non-compliant in the previous phase. The detail work in this phase are as follows:
 - a. Implementation of identified improvements in the ISMS;
 - b. Taking corrective and preventive action; applying own and other's security experiences;
 - c. Communicating activities and improvements to all stakeholders; and
 - d. Ensuring that improvements achieve the desired objectives.

Major areas for focus of ISMS

1. Security Policy

- This activity involves a thorough understanding of the organization business goals and its dependence on information system. This entire exercise begins with creation of the IT security policy. the policy should cover the following details
 - a. A definition of information security;
 - b. A statement of management intention supporting the goals and principles of information security.
 - c. Allocation of responsibilities for every aspect of implementation.
 - d. An explanation of specific applicable proprietary and general, principles, standards and compliance requirements.
 - e. An explanation of the process for reporting of suspended security incidents,
 - f. A defined review process for maintaining the policy document.
 - g. Means for assessing the effectiveness of the policy embracing cost and technological changes, and
 - h. Nomination of the policy owner.

2. Organizational Security

- This needs proper procedures for approval of the information security policy, assigning of the security roles and coordination of security across the organization.
- The main control and objectives are as follows:
 - a. Information system infrastructure: to manage information system within the organization.
 - b. Security and third party access: to maintain the security of organizational information processing facilities and information assets accessed by third parties.
 - c. Outsourcing: to maintain the security of information when the responsibility for information processing has been outsourced to another organization.

3. Assets classification and control:

- One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical sets or other similar services. This information needs to classify to indicate the degree of protection.
- The detail control and objectives are as follows
 - a. Accountability for assets: to maintain appropriate protection of organizational assets.
 - b. Information classification: to ensure that information assets receives an appropriate level of protection.

4. Personnel security

- Appropriate personnel security ensures that
 - a. Employment contracts and staff handbooks have agreed, clear wording
 - b. Ancillary workers, temporary staff, contractors and third parties are covered
 - c. Anyone else with legatine access to business information or system is covered.
- The detailed control and objectives are as follows:
 - a. Security in job definition and resourcing: to reduce the risks of human error, theft, fraud or misuse of facilities.

- b. User training: to ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in course of their normal work.
- c. Responding to security incidents and malfunctions: to minimize the damage from security incidents and malfunctions, and to monitor and learn from incidents.

5. Physical and environmental security

- Designing a secure physical environment to prevent unauthorized access, damage and interference to business premises and information is usually the beginning point of any security plan.
- Cost effective design and constant monitoring are two key aspects to maintain adequate physical security control.
- The detail control and objectives are as follows:
 - a. Secure areas: to prevent unauthorized access, damage and interference to business premises and information.
 - b. Equipment Security: to prevent loss, damage or compromise of assets and interruption of business activities.
 - c. General controls: to prevent compromise or theft of information and information processing facilities.

6. Communication and Operations management

- Properly documented procedures for the management and operation of all information processing facilities should be established. This includes detailed operating instructions and incident responses procedures.
- The detailed control and objectives are as follows
 - a. Operational procedures and responsibilities: to ensure correct and secure operation of information processing facility.
 - b. System planning and acceptance: to minimize risks of system failure
 - c. Protection against malicious software: to protect the integrity of software and info
 - d. Housekeeping: to maintain the integrity and availability of information processing and communication service.
 - e. Network management: to ensure the safeguarding of information in networks and the protection of the supporting infrastructure.
 - f. Media handling and security: prevent damage to assets and interruptions to business activity.
 - g. Exchanges of information and software: to prevent loss. Modification or misuse of information exchanged between organizations.

7. Access control

- Access to information and business procedures should be controlled on the business and security requirements. This will include defining access control policy and rules, user access management, user registration, privilege management, user password use and management, review of user access rights, network access controls, enforcing path from user terminal to computer, user authentication, node authentication, segregation of networks etc.
- The detail control and objectives are as follows:
 - a. Business requirements for access control: to control access of information
 - b. User access management
 - c. Network access control
 - d. Operating system access control
 - e. Application access control
 - f. Monitoring system access and use
 - g. Mobile computer and teleworking

8. System development and maintenance

- The detailed control and objectives are as follows
 - a. Security requirements of system
 - b. Security in application system
 - c. Cryptographic controls
 - d. Security of system files
 - e. Security in development and support process

9. Business continuity management

- A business continuity management process should be designed, implemented and periodically tested to reduce the disruption cause by disaster and security failures.
- This begins by identifying all events that could cause interruptions to business processes and depending on the risk assessment, preparation of a strategy plan.
- The main control and objective of this process is aspects of business continuity management: to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

10. Compliance

- It is essential that strict adherence is observed to the provision and international laws, pertaining to intellectual property rights, software, copyrights, safeguarding of organizational records, data protection and privacy of personal information.
- The detailed control and objectives are as follows
 - a. Compliance with legal requirements
 - b. Review of security policy and technical compliance
 - c. System audit considerations

Capability Maturity Model (CMM)

- CMM is a model of process maturity for software development which is an evolutionary model of the progress of a company's abilities to develop software.
- The CMM was designed to guide software organization in selecting process improvement strategies by determining current process maturity and identifying the few issues most critical to software quality and process improvement.
- The five levels of software maturity process are as follows:
 1. Initial : the starting point for use of a new or undocumented repeat process;
 2. Repeatable: the process is at least documented sufficiently such that repeating the same steps may be attempted.
 3. Defined: the process is defined/conformed as a standard business process, and decomposed to level 0,1 and 2
 4. Managed: the process is quantitatively managed in accordance with agreed-upon metrics; and
 5. Optimizing: process management includes deliberate process optimization/improvement.

COBIT – IT Governance Model

- COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.
- COBIT 5 is the latest edition of information system audit and control associations' globally accepted framework released in April 2012. Providing an end-to-end business view of the governance of enterprise IT that reflects the central role of information and technology in creating value for enterprise.

- **Need** of COBIT 5 in business enterprise
 1. Increased value from creation from use of IT; user satisfaction with IT management and services; reduced IT-related risks and compliance with laws, regulations and contractual requirements.
 2. The development of more business-focused IT solution and services.
 3. Increased enterprises wide involvement in IT related service.
- **Benefit** of COBIT 5
 1. Maintain high-quality information to support business decisions;
 2. Achieve strategic goals and realize business benefits through the effective and innovative use of IT;
 3. Achieve operational excellence thorough reliable, efficient application of technology;
 4. Maintain IT- related risk at an acceptable level;
 5. Optimize the cost of IT services and technology; and
 6. Support compliance with relevant laws, regulations, contractual agreements and policies.

Five principles of COBIT 5

The five key principles for governance and management of enterprise IT in COBIT 5 taken together enable the enterprise to build an effective governance and management framework that optimizes information and technology investment and use for the benefit of stakeholders.

1. *Meeting Stakeholders needs*
 - Enterprise exists to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources.
 - COBIT 5 provides all of the required process and other enablers to support business value creation thorough the use of IT.
2. *Covering the enterprise End-to-End*
 - COBIT 5 integrates governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the It functions, but treats information and related technologies as assets that needs to be dealt with just like any other assets by everyone in the enterprise.
3. *Applying a Single integrated framework*
 - COBIT 5 is a single and integrated framework as it aligns with other latest relent standards and frameworks as it align with other latest relevant standards and frameworks, and thus, allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator.
4. *Enabling a holistic Approach*
 - Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components.
 - COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help achieve the objectives of the enterprise.
5. *Separating governance form management.*
 - The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different orgnisational structures and severe different purposes.

CoCo

- The Criteria of Control model was published in 1995 by the Canadian institute of Chartered Accountant.
- CoCo describes internal control as actions that foster the best result for an organizational and those elements of an organization including its resources, system process, culture, structure and tasks that, taken together, support people in the achievement of Organization's Objective.
- The CoCo model identifies three objectives
 - a. Effectiveness and efficiency of operations;
 - b. Reliability of internal and external reporting; and
 - c. Compliance with applicable laws and regulations and internal policies.

Sys trust and Web trust

- Sys trust engagements are designed for the provision or advisory services or assurance on the reliability of system.
- Web trust engagements relate to assurance or advisory services on an organizations' system related o e-commerce.
- Following are the principles and related criteria for this Sys trust and Web trust
 1. Security: the system is protected against unauthorized access.
 2. Availability: the system is available for operation and use as committed or agreed.
 3. Processing integrity; system processing is complete, accurate and authorized.
 4. Online Privacy: Personal information obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed.
 5. Confidentiality: information designated as confidential is protected as committed or agreed.

Define the Following term

1. Information Assets register
 - IAR should be created with the details of every information assets within the organization for example.
 - a. Databases
 - b. Personal records
 - c. Scale models
 - d. Prototypes
 - e. Test samples
 - f. Contracts
 - g. Software licenses
 - h. Publicity material
 - The IAR should also describe who is responsible for each information assets and whether there is any special requirement for confidentiality, integrity or availability.
 - One major advance of this register maintain system is that in case of the password is also registered, it is a good back-up in case the carton/label containing password is accidentally misplaced.
2. **Software process capability**
 - Software process capability describes the range of expected results that can be achieved by following a software process. The software process capability of an organization provides one means of predicting the most likely outcomes to be expected from the next software project the organization undertake.
3. **Software process performance**
 - Software process performance represents the actual results achieved by following a software process. Thus, software process performance focus on the results achieved, while software process capability focuses on results expected.

4. Software process maturity

- Software process maturity is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Maturity implies a potential growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in projects throughout the organization.
- As a software organization gains in software process maturity, it institutionalizes its software process via policies standards and organizational structures.