# 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.
- 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 :

1. **The Plan Phase** - this phase serves to plan the basic organization information security, set objectives for information security and choose the appropriate security controls. Detail work in this phase are as follows:
    a. Determining 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.
    h. Obtaining management approval for residual risk.
    i. Obtaining management approval for implementation of the ISMS.
    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.

2. **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.
    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 managing security incidents.

3. **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 is as follows:
    a. Implementation of procedures and other controls for monitoring and reviewing, 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

h. Keeping records of activities and incidents that may affect the effectiveness of ISMS.

4. **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.
    c. Communicating activities and improvements to all stakeholders.
    d. Ensuring that improvements achieve the desired objectives.

**Major areas for focus of ISMS**

1. **Security Policy**
    - This activity involves a complete 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. Definition of information security;
        b. Reporting process for suspected security incidents,
        c. Specific applicable principles, standards and compliance requirements.
        d. Intention of management for supporting the goals and principles of information security.
        e. Means for assessing the effectiveness of the policy
        f. Review process.
        g. Allocation of responsibilities.
        **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
        b. Security from third party access
        c. Outsourcing

3. **Physical and environmental security**
    - Designing a secure physical environment to prevent unauthorized access, damage and interference to business premises and information.
    - 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.

4. **Human Resources Security**
    - Appropriate personnel security ensures that
        a. Employment terms and conditions are agreed up on.
        b. All users with authorized access to business information or system are covered.
        c. Temporary staff, contractors and third parties are covered

- The detailed control and objectives are as follows:
    a. **Security in job definition**: To reduce the risks of human error, theft, fraud or misuse of facilities.
    **b.** User training
    **c.** Respond to security incidents

5. **Information System development and maintenance**
    - The detailed control and objectives are as follows:
        a. Security requirements of system
        b. Security in application system
        **c.** Security of system files
        **d.** Security in development process

6. **Assets Management**
    - Information assets, (which could be software assets, physical assets or other similar services.) need to be classified to indicate the degree of Protection.
    - The detail control and objectives are as follows
        a. Accountability for assets
        b. Information classification

7. **Access control**
    - Access to information and business process should be controlled as pet the business requirements.
    - The detail control and objectives are as follows:
        a. Business requirements for access control
        b. User access management
        c. Network access control
        d. Application access control
        e. Monitoring system access control
        f. Mobile computing and tele-working
        g. Operating system access control

8. **Business continuity management**
    - It is planning for disaster and recovering from them
    - Business Continuity Management process need to be periodically tested, maintained as per the changing environment.

9. **Communication and Operations management**
    - This includes detailed operating instructions and incident responses procedures.
    - The detailed control and objectives are as follows:
        a. Protection against malicious software
        b. Operational procedures
        c. System planning: To minimize risks of system failure
        d. Housekeeping: To maintain the integrity and availability of information processing and communication service.
        e. Media handling and security
        f. Exchanges of information and software.
        g. Network management.

**10. Compliance**

- The organization should comply with application Laws and Regulation such as copyrights, 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
    c. System audit considerations

## Capability Maturity Model (CMM)

- CMM was developed by the Software Engineering Institute.
- It is a framework, designed for software developers to improve their software development capabilities.
- It provides guidance on "How to gain control on the process of developing and maintaining software.

- The **five level of software** maturity process are as follows:

1. ***Initial***
    - In the initiating level, software development processes are new and undocumented with no assurance of repeatability.

2. ***Repeatable***
    - In this level, the process is at least documented and repeatable results are expected from similar projects.

3. ***Defined***
    - An improvement form the repeatable phase, defined process and procedures are in place and used.

4. ***Managed***
    - In this process is quantitative data is collected and analyzed. A improvement program is used for improving software productivity and reaching zero defects goals.

5. ***Optimizing***
    - At this point a process of continuous improvement occurs.

## COBIT 5

- COBIT stand for **C**ontrol **Ob**jective for **I**nformation and Related **T**echnology.
- COBIT 5 is the latest edition of ISACA, globally accepted framework released in April 2012.
- COBIT 5 is the business framework for the governance and management of enterprises IT.
- The principles, practices, tools and models found in COBIT 5 represent the collective wisdom of global IT and governance experts.

➢ **Need of COBIT 5**

- ➢ More Business Focused
- ➢ Achieve Strategic goals
- ➢ Compliance with rules and regulation
- ➢ High Quality information
- ➢ Operational Excellence
- ➢ Greatly improves business outcome
- ➢ Increased user satisfaction
- ➢ Reduced IT related risks.
- ➢ Lower IT cost.

- **COBIT 5 Enablers**
    1. Principles, Policies and Framework
    2. Processes
    3. Organization Structures
    4. Culture, ethics and behavior of individuals
    5. Information
    6. Service, Infrastructure and Application
    7. People, Skills and Competencies

**Five principles of COBIT 5**

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 through the use of IT.

2. *Covering the enterprise End-to-End*
    - COBIT 5 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.

3. *Applying a Single integrated framework*
    - There are so many IT-related Standards and best practices, each providing guidance for IT activities. COBIT 5 aligns with them to simplify the complexity.

4. *Enabling a holistic Approach*
    - 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 from management.*
    - The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines involved different types of activities serve different purposes and require different organizational structures to fulfill their individual needs.

**CoCo**

- The Guidance of Control Report known as CoCo was published in 1995 by the Canadian institute of Chartered Accountant to translate COSO into practical implementable activities.
- As per CoCo internal control are those elements or process which help organization to achieve goal and objective.
- The CoCo model identifies **3 objectives**
    1. Effectiveness and efficiency of operations.
    2. Reliability of financial reporting.
    3. Compliance with applicable laws and regulations.

**Sys trust and Web trust**

- **Sys trust**: It is an assurance service that independently tests and verifies system reliability.

- **Web trust**: It relates to assurance service of an organization's system related to E-commerce security.

- **Principles and related criteria** for this Sys trust and Web trust.
    1. Security
    2. Online Privacy
    3. Confidentiality
    4. Availability
    5. Processing integrity

## ITIL (Information Technology Infrastructure Library)

- It consist a series of books which provides a set of best practice guidelines in the management of IT service.

- The **Details of ITIL Framework/ 5 Service Lifecycle Stages** are as follow:

    1. ***Service Strategy***
        - This volume deals with the strategic management approach in respect of IT Service Management.

    2. ***Service Design***
        - It provides procedures for design of new services as well as design of existing service improvement.

    3. ***Service Transition***
        - It includes procedures for testing and validating the services prior to moving the service in to productions.

    4. ***Service operation***
        - It includes procedures for resolving customer problem, fixing IT failure immediately etc.

    5. ***Continual Service Improvement***
        - In this stage, IT organization collects data and feedback from users, customers, stakeholders and other sources to enhance services to ensure that a service delivers the maximum benefits.