School of Computer Science and IT
JAIN (DEEMED-TO-BE UNIVERSITY)
Department of Bachelor of Computer Applications

# Module 5

# Information Security Management

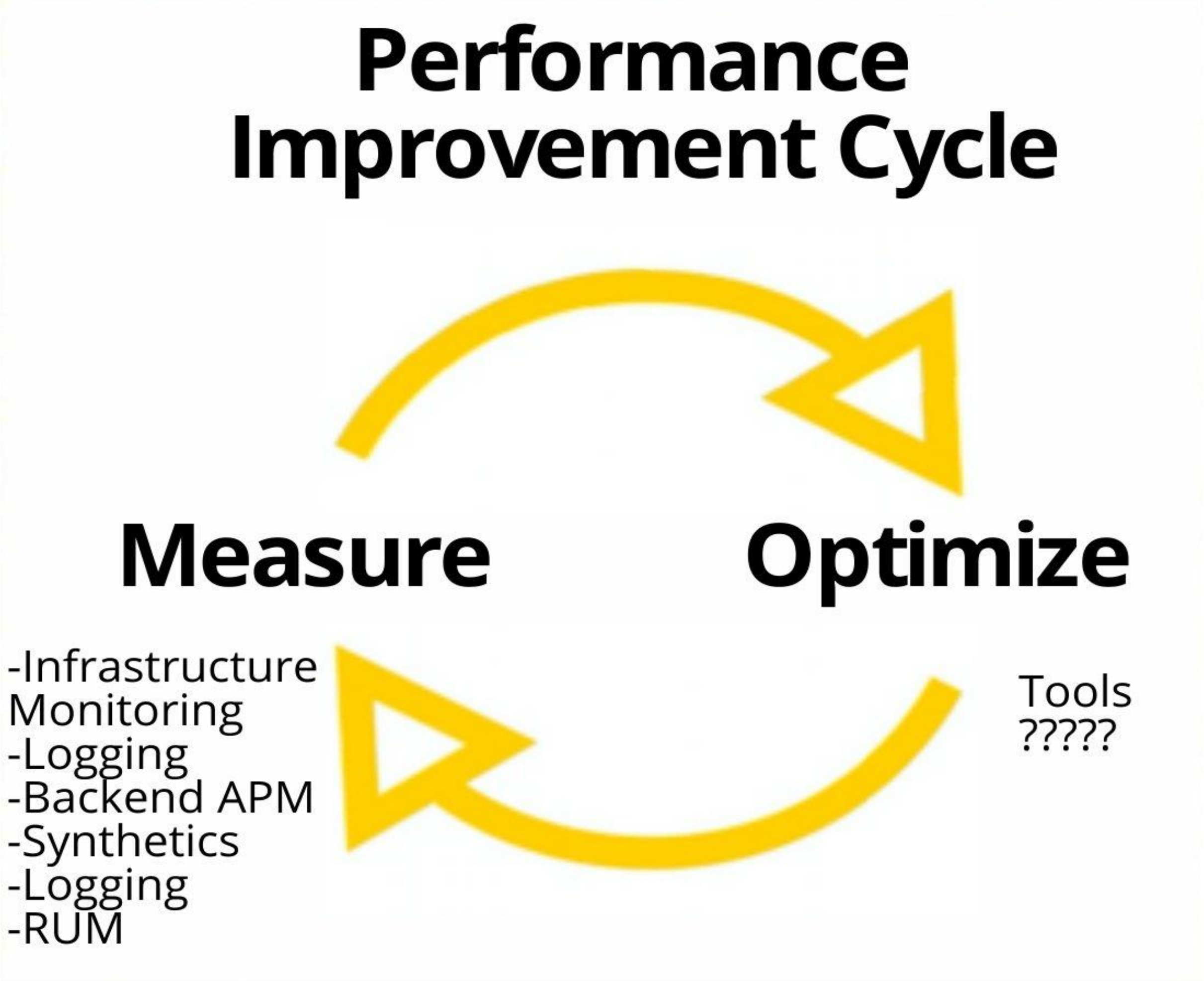
Dr. Ajay Shriram Kushwaha

# Agenda

- Introduction
- ISMS Framework
- IT Security roles & responsibilities
- Segregation of Duties
- Description of COBIT and other Frameworks

# Performance Optimization

- Refer Security Metrics  Program in Module 3 Last topic



# Segregation of Duties

1. **Legal Owner** : The top management shall be legal owner of information asset. No individual can claim IP rights of an Information asset, unless and otherwise specifically agreed and approved by the management in contractual agreement.
2. **Delegated Ownership** : The CEO shall have authority to represent the organization for the protection and security of the information asset as ownership of Information assets is delegated to this organizational role. CEO shall approve the Information Management / Security Policy.

# The responsibilities of the Asset owner are as follows:

- Updating of information asset inventory register;
- Identifying the classification level of information asset;
- Defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of the information asset;
- Assessing and monitoring safeguards to ensure their compliance and report situations of non-compliance;
- Authorizing access to those who have a business need for the information, and
- Ensuring access is removed from those who no longer have a business need for the information.

# 3.Chief Information Officer

- The CIO ensures that strategic planning processes are undertaken.
- The CIO ensures that information security policies and governance practices are established to ensure the quality and integrity of the agency’s information resources and supporting IT systems.
- They oversee the development of tools, systems and information technology infrastructure to maximize the access and use of an agency’s information resources.

# Contd..

- The Chief Information Officer is responsible for:

- Interpreting the business and information needs and wants of the organization and translating them into ICT initiatives
- Setting the strategic direction for ICT and information management
- Ensuring that ICT and information management investment is aligned to the strategic goals of the organization
- Ensuring that projects and initiatives are aligned and coordinated to deliver the best value
- Ensuring ICT planning is integrated into business planning
- Identifying opportunities for information sharing and cross collaboration on projects and initiatives.

# 4. Information Security Officer

- The information security officer is responsible for developing and implementing information security policy designed to protect information and any supporting information systems from any unauthorized access, use, disclosure, corruption or destruction.
- The information security officer shall:

- ➢ Develop policies, procedures and standards to ensure the security, confidentiality and privacy of information that is consistent with organizational Info security policy
- ➢ Monitor and report on any information intrusion incidents and activate strategies to prevent further incidents.
- ➢ Work with information custodians to ensure that information assets have been assigned appropriate security classifications.
- ➢ Maintenance and upkeep of the asset as defined by the asset owner
- ➢ Implementing any changes as per the change management procedure
- ➢ Backup of the information
- ➢ Authorizing access to those who have a business need for the information

# 5. Data Operators / End Users Employees

- Third Parties, Contractors authorized by the Owner / custodian to access information and use the safeguards established by the Owner / custodian.
- Being granted access to information does not imply or confer authority to grant other users access to that information.
- The users are bound by the acceptable usage policy of the organization.

# Description of COBIT and other Frameworks

- **Explain about COBIT, Val-IT and Risk IT Framework**

Definition : **Control Objectives for Information and Related Technology**

- **COBIT** is a framework for developing, implementing, monitoring and improving information technology (IT) governance and management practices. The **COBIT** framework is published by the IT Governance Institute and the Information Systems Audit and Control Association (**ISACA**).

Why COBIT?

- It is a framework created by the ISACA (Information Systems Audit and Control Association) for IT governance and management. ... Overall, **COBIT** ensures quality, control, and reliability of information systems in organization, which is also the most **important** aspect of every modern business

**Purpose :**

- The purpose of COBIT is to provide management and business **process** owners with an information technology (IT) governance model that helps in delivering value from IT and understanding and managing the risks associated with IT.

# Security Program Effectiveness

- Retaining or increasing information security resources requires us to quantify the benefits provided to the organization.
    - Business leaders understand metrics.
    - Sales people are held to revenue targets.
    - Network administrators are held to uptime guarantees.
    - Customer service representatives are held to satisfaction scores.
    - Information security professionals can meet similar, measurable standards

# Contd..

- There are four areas that can help quantify information security's contribution to an organization.
  - Audit Results
  - Taking a risk based approach
  - Communication is key
  - Lost Productivity
  - User Satisfaction
  - User Awareness
- https://searchsecurity.techtarget.com/tip/Four-ways-to-measure-security-success
- https://www.infosecurity-magazine.com/opinions/how-measure-effectiveness-security/

# Continuous Assessment and Improvement

- In a changing environment, the success of an organization has become closely related to its ability to manage risks.
- The increasing variety of threats and ferocity attacks make the protection of information assets a complex challenge.
- Ensuring information security becomes a necessary condition for the sustainable progress of the organization at least for the following reasons :
    - Maintaining competitive advantage
    - Protect reputation
    - Ensure compliance with applicable laws and regulations

# Contd..

- self-assessment for continual improvement of information security management:

Two main directions were investigated:

- Auditing techniques and methodologies : As a driver for continual improvement inside the Plan-Do-Check-Act cycle for continuous improvement
- Process maturity/capability models : As a driver for achieving compliance with requirements

Approaches Used for assessment and continuous improvement of ISM :

- The reference standard for information security – ISO/IEC 27001:2013 (ISO, 2013), uses the established Plan-Do-Check-Act approach to drive continuous improvement.
- This approach, auditing is the managerial tool which provides stakeholders with reasonable confidence in the achievement of organizational goals

# Contd..

- Maturity evaluation models are a structured sets of criteria that describe the capability of an organization's behaviors and processes to produce the desired results in a reliable and sustainable manner (ISO, 2008).

Three complementary models for assessing security maturity:

- The International Standards Organization's Systems Security Engineering Capability Maturity Model (ISO, 2008) - focuses on security practices and evaluates maturity by means of their reliability and sustainability, ranging from informal practices to defined, controlled and continuously improving practices.
- The federal information security technology assessment framework (NIST, 2013) : focuses on policies, procedures and technical controls, and their implementations
- Control Objectives for Information Technology – COBIT (IT Governance Institute, 2007): ) focuses on risk management; information security maturity is appraised by the capability of the associated risk management framework

# Continuous security management

- Based on enterprise requirements and business type, we will:
    - Identify security requirements at the design phase level
    - Identify security functions based on the solution type
    - Use known, bug-free and vulnerability free technologies
    - Recommend environment security setup
    - Monitor and manage security configurations
    - Employ testing strategies to confirm solution security posture
    - Continuously monitor vulnerability alerts
    - Apply patches for vulnerability alerts when available

# Outsourcing Versus In-sourcing

- The primary variation between outsourcing and in-sourcing is the method in which work is divided between various companies or departments for strategic purposes.
- Assigning a project to a person or department within the company instead of hiring an outside person or company to do the work is considered insourcing.
- Outsourcing is usually done as a cost-cutting measure. It can affect jobs ranging from customer support to manufacturing, as well as technology and the back office.

Here are the key differences between the two business practices:

- Cost
- Resources
- Control
- Location

Outsourcing Versus In-sourcing
https://www.investopedia.com/ask/answers/032715/whats-difference-between-outsourcing-and-insourcing.asp

# Impact of ISM program across organization

**What is an ISMS?**

- An **information security management system**(ISMS) is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.
- It can help small, medium and large businesses in any sector keep information assets secure.
- An ISMS is a set of policies concerned with information security management or IT related risks.
- An organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets.
- An ISMS must remain effective and efficient in the long term, adapting to changes in the internal organization and external environment.

# Why do we need an ISMS?

Security experts say:

- Information technology security administrators should expect to devote approximately one-third of their time addressing technical aspects.
- The remaining two-thirds should be spent developing policies and procedures, performing security reviews and analyzing risk, addressing contingency planning and promoting security awareness;
- Security depends on people more than on technology;
- Employees are a far greater threat to information security than outsiders;
- The degree of security depends on three factors: the risk you are willing to take, the functionality of the system and the costs you are prepared to pay;
- Security is not a status or a snapshot, but a running process.
- These facts inevitably lead to the conclusion that **security administration is a management issue, and not a purely technical issue**

# PDCA model

- ISMS incorporates, the "Plan-Do-Check-Act" (PDCA) approach:

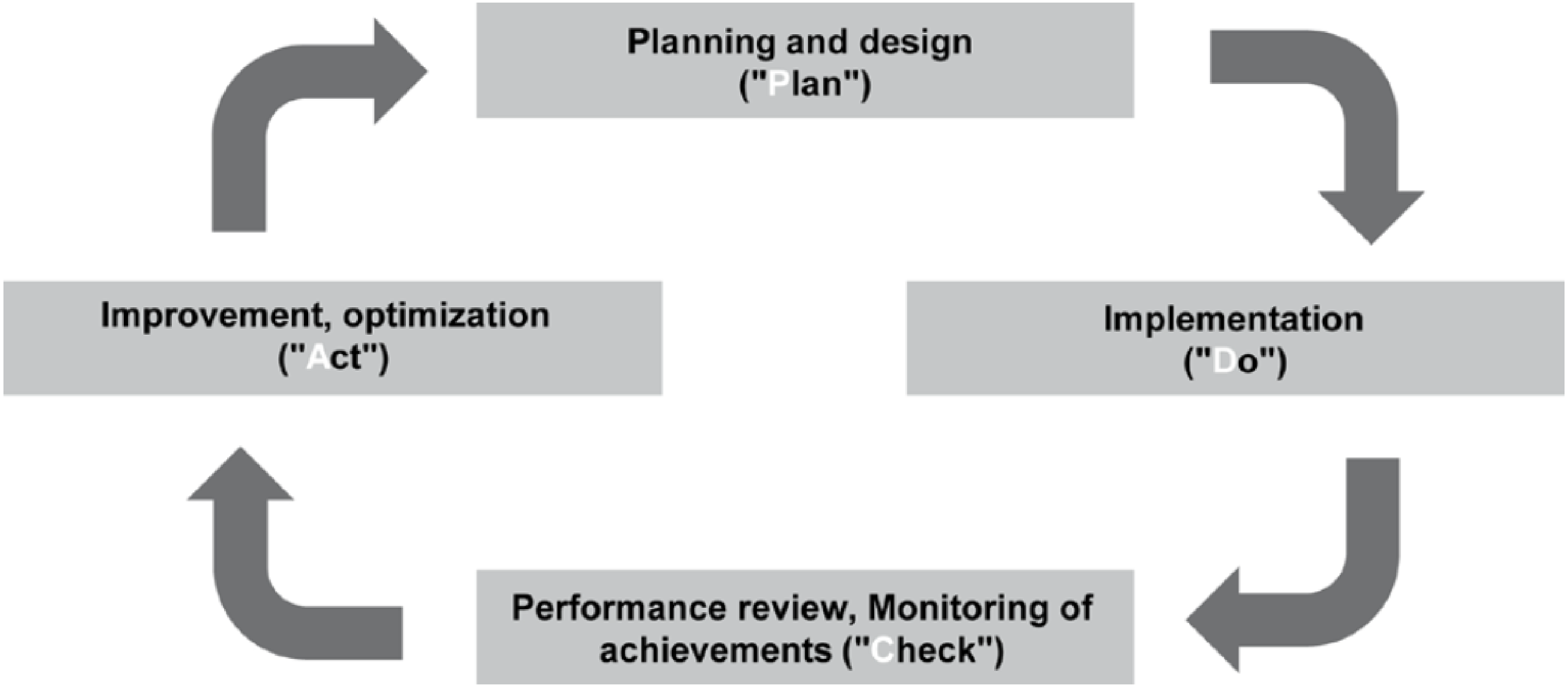
1. The **Plan** phase is about designing the ISMS, assessing information security risks and selecting appropriate controls.

2. The **Do** phase involves implementing and operating the controls.

3. The **Check** phase objective is to review and evaluate the performance (efficiency and effectiveness) of the ISMS.

4. In the **Act** phase, changes are made where necessary to bring the ISMS back to peak performance.

# PDCA Model



Planning and design ("Plan")

Implementation ("Do")

Performance review, Monitoring of achievements ("Check")

Improvement, optimization ("Act")

# CIA

- The establishment, maintenance and continuous update of an ISMS provide a strong indication that a company is using a systematic approach for the identification, assessment and management of information security risks.

**Critical factors of ISMS:**

**Confidentiality**: Protecting information from unauthorized parties.

**Integrity**: Protecting information from modification by unauthorized users.

**Availability**: Making the information available to authorized users.

# CIA

- A company capable of successfully addressing information CIA requirements which in turn have implications:

  1. Business continuity;

  2. Minimization of damages and losses;

  3. Competitive edge;

  4. Profitability and cash-flow;

  5. Respected organization image;

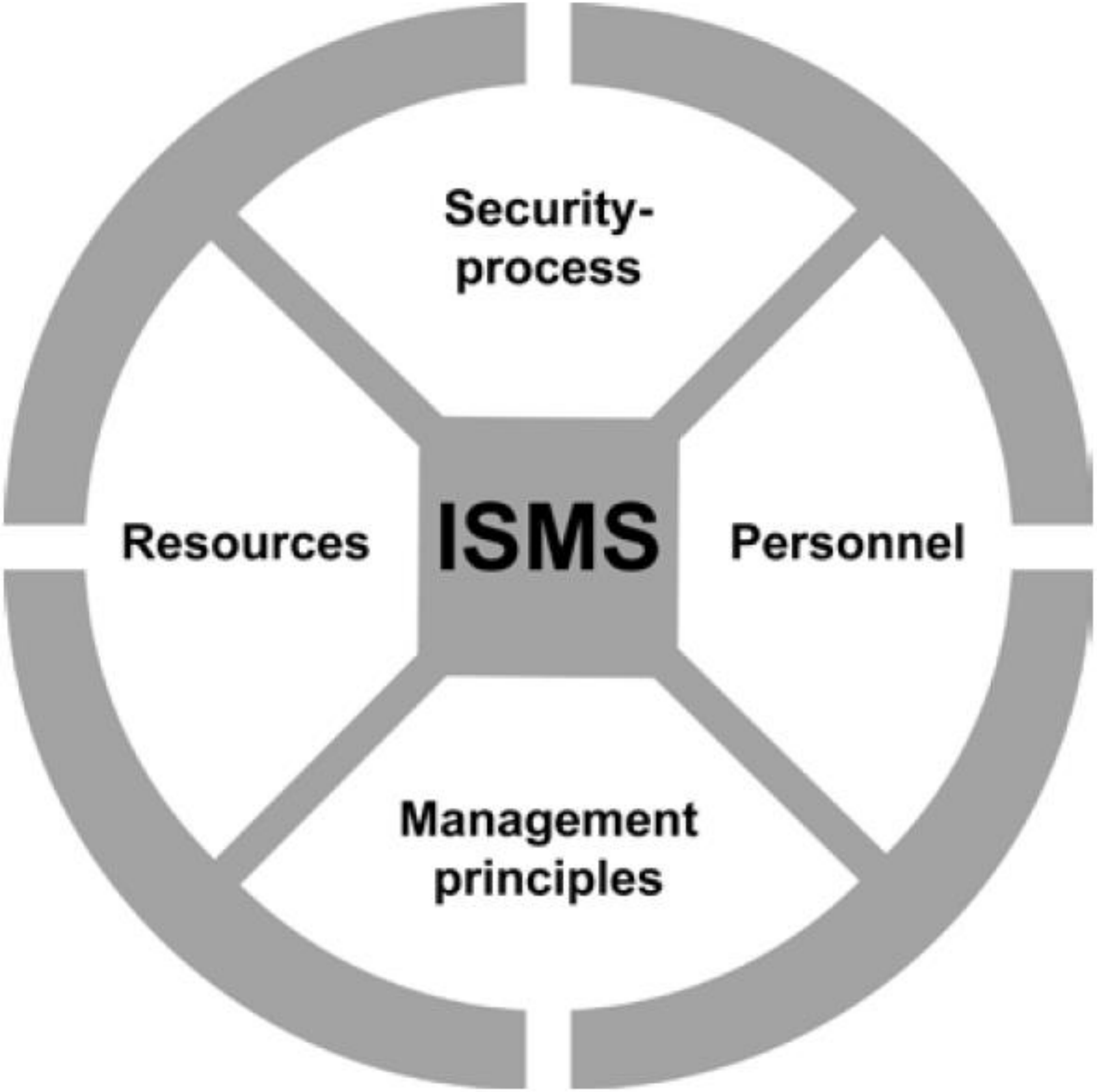
  6. Legal compliance

# Components of ISMS

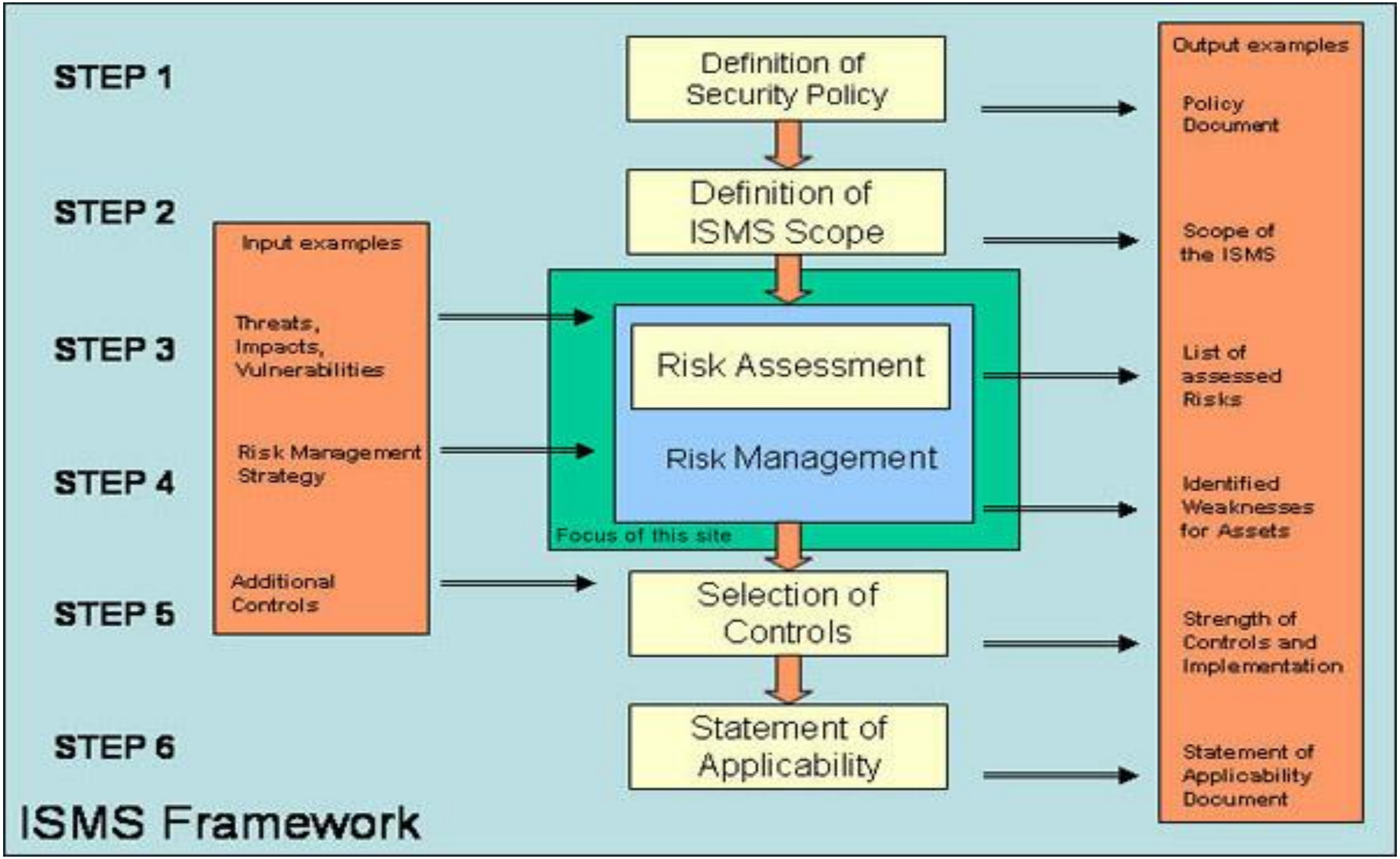
ISMS involves the following essential components :

- Management principles
- Resources
- Personnel
- Information security process:
  - Policy for information security in which the information security objectives and strategies for their implementation are documented
  - Information security concept
  - Information security organization - Information security organization and security policy are the tools that the management uses to implement its security strategy.

# Components of ISMS



# ISMS Framework



# ISMS framework

- Developing an ISMS includes the following steps:

  1. Definition of Security Policy,

  2. Definition of ISMS Scope,

  3. Risk Assessment (as part of Risk Management),

  4. Risk Management,

  5. Selection of Appropriate Controls and

  6. Statement of Applicability

- Security policy is the demonstration of management’s intent and commitment for the information security in the organization. And provide direction to the information security efforts of the organization.
- The ISMS scope is to define which information you intend to protect.

# Framework

- Steps 3 and 4, the Risk Assessment and Management process, comprise the heart of the ISMS.
- They "transform" the rules and guidelines of security policy and objectives of ISMS into specific plans for the implementation of controls and mechanisms that aim at minimizing threats and vulnerabilities.
- Steps 5 and 6 are rather related to the operative actions required for the technical implementation, maintenance and control of security measurements.
- Appropriate controls may either be derived from existing sets of controls or mechanisms, usually included in information security standards and guidelines
- Or a combination or adaptation of proposed controls to the specific organizational requirements or operational characteristics.
- In both cases, step 6 is the documented mapping of the identified risks, applied to the specific organization with the technical implementation of security mechanisms the organization has decided to deploy.

# Establish Wireless Lan Security Policies And Practices

- The cornerstone of an effective wireless LAN strategy involves defining, standardizing, documenting, disseminating, and enforcing wireless LAN security policies and practices.
- These include specifying the make, model, configuration, and settings of the wireless LAN equipment authorized for use, as well as documenting and managing the APs and connected network infrastructure.
- Employee education increases awareness of security risks. Some employees may not realize that deploying an unauthorized wireless LAN or using a WiFi product “out of the box” may increase security risks. Clear and frequently conveyed guidelines usually promote active cooperation.
- DESIGN FOR SECURITY When placing wireless APs for strategic coverage, installers should consider signal bleed into uncontrolled areas where transmissions can be intercepted. Wireless coverage should be implemented only where needed.
- LOGICALLY SEPARATE INTERNAL NETWORKS The LAN segments that connect to wireless APs should connect to a corporate Virtual Private Network (VPN) gateway, but not directly to the production network. Eliminating APs from the production network minimizes the risk of attack techniques such as packet sniffing.

# Contd.,

- ENABLE VPN ACCESS ONLY Requiring users to connect to the wireless LAN via a VPN is recommended. Once authenticated, authorized users communicate using an encrypted tunnel between the connecting device and the LAN, reducing the risk that a transmission will be captured.
- RESTRICT UNNECESSARY PROTOCOLS Restricting unnecessary or redundant protocols from the LAN segments that connect the APs to the VPN gateway reduces the possibility of unidentified holes and vulnerabilities. Retaining the Domain Name System (DNS) and IP Security (IPSec) protocols is recommended to support the VPN.
- RESTRICT AP CONNECTIONS Administrators can use authorization tables to selectively enable LAN connections only to devices with approved NIC addresses. Each NIC has a unique address that can be added to a table of authorized users; most vendors' APs support Media Access Control (MAC) restrictions through the use of authorization tables. As a result, instead of editing each AP individually, APs can be pointed to a centrally managed database.

# Contd.,

- PROTECT WIRELESS DEVICES Personal firewalls can protect individual devices from attacks launched via the “air connection” or from the Internet. IT administrators should disable all unused features of new client devices (e.g., shared drive access) and reconfigure default settings according to the organization’s particular needs.

Feel Free to ask for Any query

Ajay Shriram Kushwaha