STUDY GUIDE FOR MODULE NO. 2

Unit 2 – Information Assurance Planning

MODULE OVERVIEW

This module examines the practical considerations made when planning and establishing an information assurance management program. It starts with the approaches to implementing information assurance, followed by discussing the possible structures that may be adopted by an organization to implement the information assurance management system. We will also discuss the asset management and gets into the fundamental processes of risk management and how best to implement it across an organization. Following this, is the explanation of organizational information assurance policy.

MODULE LEARNING OBJECTIVES

At the end of this, students are expected to:

1. Describes approaches for implementing information assurance and the importance of an organization's information assurance policy.
2. Discuss the possible structures that may be implemented by an organization to implement the information assurance management system
3. Discuss the risk management process.
4. Explain the importance of policy.

LEARNING CONTENTS (Approaches to Implementing Information Assurance)

In implementing an information assurance program, the approach taken also plays an important role. Organizations can use a top-down or bottom-up approach to implement and execute information assurance. Selecting a suitable approach depends on an organization's requirements. Sometimes a hybrid is the right decision. For example, a large multinational organization with branches in different countries might select a top-down approach to match general corporate security requirements, while the bottom-up approach is used at the same time to meet local security requirements within specific economies.

Key Components of Information Assurance Approaches

1. **People**

   People are a challenging and crucial resource that need management. By applying the right processes and technology, people add value to organizations. When implementing the technology and operating the processes, an organization should have trained the right employees to maximize the efficient use of the technology. Awareness, training, and education are key to making information assurance work.

2. **Process**

   Process refers to the use of a formalized sequence of actions to achieve an aim. For example, recruiting new employees has its own process beginning with the advertisement stage and ending with the actual hiring. As an organization matures, processes or procedures should become more efficient and discriminating over time. Legal, regulatory, and contractual requirements and obligations are matters that should be weighed in terms of their impacts to current processes.

3. **Technology**

   The technology component requires examining the hardware, software, and physical facilities to ensure better operations and execution of the computer security processes. Large organizations may spend money for operational problems created by implementing technological solutions without a plan. However, smaller organizations do not have the same resources. Therefore, it becomes riskier when

you make an inappropriate selection. An organization should ensure the hardware or software purchased is cost-effective, meaningful, and useful.

A common approach for those beginning to implement an information assurance capability is to focus on technology. This often leads to the purchase of several information assurance tools such as vulnerability scanners, penetration testing systems, and intrusion detection systems.

Another approach could include hiring information assurance employees, directing them to write policies, standards, and procedures for the secure handling of information, and having them perform a risk assessment. Using the results from the risk assessment, the organization could then determine the best requirements for technology. Purchase technology that meets a specific need of the organization (such as encryption for the banking or healthcare industry) and targets a specific risk. Now the risk of a breach (which can be extensive in terms of monetary and reputation loss) is reduced through procedures and technology.

Levels of Controls in Managing Security

An important element of a security program is the collection of controls that an organization needs to have in place. Because each organization is unique, every security program is different. Even though security programs are different, they are composed of the generic elements shown in Figure 2.1.

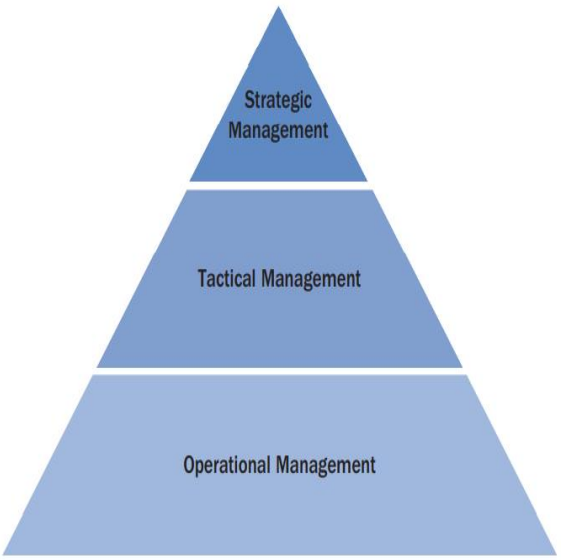


Fig 2.1 Levels of controls in an information assurance program

Strategic management includes security processes such as conducting risk management exercises, security awareness programs, policy development, and compliance efforts with laws and regulations.

Tactical management examines business continuity, data classification, process management, personnel security, and risk management.

Operational management includes areas of communication security, security of an information system life cycle, and incident response.

Top-Down Approach

- In this approach, senior management shows that it takes security seriously and is actively involved in spreading information assurance awareness. They should mandate observation of the information assurance policy. This way, security is not just a matter of technology or an antivirus or firewall solution, which is often a result of lack of awareness in information security.
- A top-down approach is characterized by a high degree of control from the head office. It includes the overall strategy of its approach and phases of implementation. This approach encourages integration. It is easier to combine different elements in an information assurance program when it receives demonstrated support from the highest management level.

Bottom-Up Approach

- A bottom-up approach refers to a situation in which a functional department or unit adopts strategic, operational, or tactical management to develop a security program without senior management support and direction (see Figure 2.1). A bottom-up approach is good for areas in organizations that need immediate security attention because of high risk or available budget. Since this approach focuses fully on technology or operational controls, it is more effective by addressing daily operational requirements.

- The bottom-up approach is better when there is clear indication that implementers' resistance to change stems from insecurity such as anxiety about losing jobs because of a potential merger. Linking the elements in a bottom-up approach creates a larger process, part, or system, which is effective for faster integration. In using this approach, the challenge is to gain the support of senior managers to drive process improvement forcefully among subordinates.

Finally, organizations should protect not only their own and customers assets but also associated brands, networks, and web sites. All online content, communication, and commerce should be protected within every layer of data transmission and storage proportionate to the value of the data. End-to-end security is not only necessary to preserve customer confidence and encourage online usage, but also to avoid regulatory penalties, financial liabilities, and consequential losses. End-to-end security refers to a situation where information from the sender is being encrypted and secured from the moment it is created, stored, and transmitted, until it is received at the destination.

LEARNING CONTENTS (Organizational Structure for Managing Information Assurance)

Information assurance is an interdisciplinary and multidepartmental issue requiring commitment from the entire organization.

Importance of Managing Information Assurance as a Program

A well-planned information assurance management program produces the following positive results:

- It will have continuous support and commitment from the top management to sustain an effective program by ensuring matters such as required resources are available.
- Employees will be directly involved in the planning of local security systems.
- Executives will have a better understanding of the organization and will be able to effectively play their role and use their authority to protect information.
- Information assets will be securely managed by the organization as per information handling categorization.
- Managers within each of the business and operational units will be more aware and familiar with specific security requirements, including technical and procedural requirements, associated challenges, and risks of the IT environment.
- It will implement secured physical and logical access to IT infrastructure.

Structure of an Information Assurance Organization

There are three types of structural options available for consideration.

1. **Centralized structure** where an information assurance management program is managed under a centralized unit with ultimate accountability and responsibility for the program.
   Some examples of activities that should be centralized include the following:
   a. Defining information assurance roles, responsibilities, and authorities
   b. Developing IT security architecture
   c. Developing policies and guidelines
   d. Organizing an awareness program
   e. Setting up a computer emergency readiness team (CERT) capability and conducting training for the selected personnel
2. **Distributed structure** where roles, responsibilities, and authorities are spread throughout the organization's business units, operations areas, and geographical locations. each functional unit (department, division, subsidiary, or business location) is responsible for its own security planning and implementation.
3. **Hybrid structure** that is a mix of the centralized and distributed structures. The hybrid structure features centralized management of information assurance with decentralized execution of security activities. From a practical perspective, a hybrid structure attempts to avoid redundant tasks and waste of resources. The centralized part promotes uniformity in activities across the organization while the distributed part allows for easier enforcement of policies and internal regulations across the organization.

Information Assurance Staffing

In addition to the basic elements in an information assurance management structure, recruiting and assigning the right personnel to handle information assurance–related jobs are vital tasks.

Industry has established a generic list of the main groups that an organization should involve in the information assurance management program structure.

1. **Senior management**

In addition to accepting risk and setting direction, senior management establishes and enforces the organization information assurance program. They endorse and approve policies and objectives supporting the vision and mission of the organization, define and appoint, or change the roles and responsibilities of the appropriate management representatives and the tactical security team members.

2. **Information assurance units**

An information assurance unit directs, coordinates, plans, and organizes information assurance activities organization wide. The unit communicates relevant security matters to both internal and external parties as appropriate. The unit works with a variety of individuals, bringing them together to implement controls in response to current and anticipated information assurance risks.

This unit is also in charge of suggesting strategy and taking steps to implement the controls needed to protect both the organization's information and the information supplied to the organization by external parties. More importantly, it investigates ways that information assurance–related technologies, requirements, processes, and organizational structures are applied to achieve the goals of the organization's strategic plan.

3. **Information security units**

The information systems security officer (ISSO) is an individual responsible for ensuring that the appropriate operational assurance posture is maintained for an information system and as such works in close collaboration with the information system owner.

The information system security officer often plays an active role in the monitoring of a system and its environment of operation, which includes developing and updating the system's security plan, managing and controlling changes to the system, and assessing the security impact of those changes.

4. **Technology and service providers**

Technology and service providers supply information assurance consultancy, services, and products.

Technology Providers	Security Responsibilities
Programmer	• Develop systems/software in accordance with specifications set • Ensure that secure programming practices are observed
Help desk	• Act as a first liner in attending to users' complaints and security-related incidents • Escalate the security incidents to the information assurance unit for further review or investigation
Database administrator	• Implement access control for databases •Take part in user access management such as sanctioning •Implement controls to ensure confidentiality, integrity, and availability of data in the database • Monitor database activities to track potential security violation or performance issues
System/network administrator	• Configure a system and network in accordance with security specifications set by the information assurance unit • Patch and update the system to ensure that it is free from vulnerabilities
Information systems/ business analyst	•Ensure that adequate controls are implemented during the application development life cycle •Ensure that security requirements are incorporated during system design and development •Include suitable controls in all proposed information system solutions

5. **Supporting functions**

Supporting Function	Security Responsibilities
Physical security/facility management/property management	Develop and enforce appropriate physical security controls, with input from information assurance management and other relevant parties

Human resource department/unit	• Conduct screening and background investigation for an identified position • Coordinate and provide security training and awareness to employees • Ensure compliance with labor law and relevant legislation • Take part in all personnel-related matters such as definition of terms and conduct of employment, performance evaluation, and career path planning
Audit	• Perform compliance checking and ensure compliance with relevant laws, regulations, or policies • Review effectiveness of internal control and implementation of information assurance
Legal	• Ensure compliance with relevant regulations and legislations • Ensure security requirements are incorporated in contracts and agreements • Provide advice on legal matters
Risk management	• Develop a risk mitigation plan • Identify and evaluate risks inherent in the organization including security-related risks • Responsible for contingency planning for the organization • Review effectiveness of internal controls in mitigating identified risks

6. Users

Types of User	Security Responsibilities
Users of information	People, organizations, or other entities that are "consumers" of the services of the information system. Sometimes they directly interact with the information system (for example, to print a report from the system). Otherwise, they may read only information system–generated reports or be briefed on such items. Users of information normally know what their needs are regarding the confidentiality, integrity, or availability of the information.
Users of systems	Individuals who directly use an information system and whose duties are to follow information assurance procedures, attend required information assurance training courses or programs, and report any security problems

LEARNING CONTENTS (Asset Management)

A best-practice security risk assessment exercise begins with an identification of the assets, followed by an evaluation of the asset sensitivity and criticality. This ensures that asset protection is proportional to the asset value.

Assets are tangible or intangible. Tangible assets range from data files to physical assets, such as computer peripherals, while intangible assets include the image and reputation of the organization, general utilities, and skill sets of a workforce.

Types of Assets

Types	Examples
Data/information	Databases, personnel records, proposals, contracts, manuals, statistics, and any data/information in either soft or hard copy lighting Software Application software, system software, system utility, development tool
Hardware	Computer/network equipment, tape, removable media

Intangible	Reputation, image, influence, intellectual property
People	Staff with expertise, skill, and knowledge on a subject
Service	Electricity, telecommunication service, lighting
Software	Application software, system software, system utility, development tool

Tangible asset values can be quantified for the organization. For example, a server has a certain monetary replacement cost. This cost is part of its value. Next, the server is critical for providing e-commerce billing services to an organization's web site. If it is down, the organization loses money for every missed sale. This is also a quantifiable value and can be added to the server's total value. Finally, the configuration of the server may be proprietary or an industry trade secret. While the research used to develop the server configuration has a cost, if the proprietary configuration were stolen, the impact to the company because of increased competition could be immeasurable or extremely hard to quantify and therefore intangible.

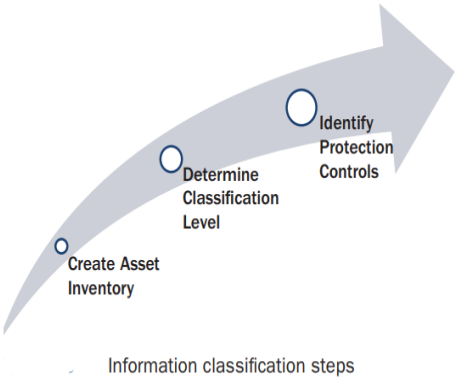
Responsibilities for Assets

Asset responsibility provides accountability for the protection of the assets under the individual's control. Protection includes appropriate information assurance and access control failures resulting in unauthorized access to and use of the assets. Three controls are required to assign responsibility: inventory of assets, ownership of assets, and acceptable use of assets.

1. **Inventory of assets**
   The organization establishes a baseline by identifying and recording important information about assets such as their location, license information, and security classification or categorization. Placing data into categories is the core of the asset management process, which ensures that movement of assets and changes to its information are documented and updated regularly.
2. **ownership of assets**
   It is important to establish that each asset has an assigned owner. The owner ensures that assets are classified properly, and asset use authorizations are reviewed periodically. The owner can delegate the implementation of information assurance to someone else; however, the overall accountability remains with the owner.
3. **acceptable use of assets.**
   To protect organizational assets, develop and document policy and guidelines for acceptable asset use. Ensure that the policy is endorsed by senior management. The policy elaborates on the rules and responsibilities of asset usage by internal and external parties in accordance with the security classification of the asset.

- Protecting information assets is resource intensive; ensure the investment made is cost-beneficial to the organization. Conducting an information classification exercise ensures that data is protected cost-effectively. To achieve these objectives, two controls should be in place, namely, classification guidelines and information labeling and handling.
  a. **classification guidelines**

Organizations must perform the classification process on a regular basis to consider the life cycle of the information and its application. The life cycle starts from the creation of information, implementation of the access control, method of processing, and eventually information disposal. The access control associated with the classification should comply with the access control policy of the organization.



Information classification steps

b. information labeling and handling

A proper and structured labeling scheme and handling mechanism is essential to secure and preserve an organization's information assets. Information may be handled between different organizations, different components within an organization, or even different security levels within a system.

An organization should develop detailed information handling procedures derived from the organization's policy on classification. For confidentiality, most organizations have adopted four levels of information classification: secret, confidential, restricted, and public. Other classifications are used for integrity and availability. The definitions of the classification and methods of processing, transmission, storage, accessibility, and disposal have to be documented by the organization. The procedure should cover physical assets and information kept or transferred in electronic formats such as e-mails and paper documents. Properly labeled assets encourage better handling and management by employees and partners.

LEARNING CONTENTS (Information Assurance Risk Management)

Information assurance risk management is essential for an effective information assurance management program. It is integral to good management practice.

Risk management refers to the application of a method that consists of policies, procedures, and practices used to identify these risk events. The objective is to identify, analyze, treat, evaluate, and continue to improve the way the organization manages its risk profile. In short, risk management is a means to identify, manage, and control risk.

Risk management process

Risk Management Process

1. Background planning

- Establish the aim, scope, and boundary.
- Establish the risk evaluation criteria.
- Establish risk management policy.

2. Asset analysis

- The process of asset analysis is often conducted in parallel or as part of asset valuation. Organizations identify the significant assets within the scope of

assessment and analyze their values in terms of confidentiality, integrity, and availability. These assets will be analyzed based on their types, such as software, hardware, people, service, and platforms.

- Determine the value of the asset in terms of the following:
  • **Confidentiality** (consider the loss or harm that would result from unauthorized disclosure of the asset or of the information handled or protected by the asset).
  • **Integrity** (consider the loss or harm that would result from unauthorized modification of the asset).
  • **Availability** (consider the loss or harm that would result from partial or total unavailability of the asset).

3. Threat analysis

The goal of this analysis is to identify and examine threats to each asset, respectively. Threat analysis is the most difficult aspect of risk analysis. Threat information is not limited to merely actors who may want to steal an organization's information but also actors who may want to damage an organization or have a personal vendetta against an organization's employees or partners.

Categories of Threats

a. Human Threats

- **Motive** - Why is a person motivated to perform an act? Common motivations are control, curiosity, duress, fame, monetary gain, nationalism, power, and revenge.
- **Means** - describes the ability to execute the motivation. Some may try to find individuals who have the means to perform the action on their behalf.
- **Opportunities** - These represent the actual moment in time when a motivated actor with means could execute an action. Opportunities may be the physical presence of an individual in a vulnerable location or may be a newly discovered firewall vulnerability.
- **Accidental actions** are another type of human threat. Accidental actions are caused by carelessness, errors, and sometimes inadvertent omissions.

b. Natural threats

- Examples of natural threats are weather-related phenomenon (such as hurricanes, tornados, and flooding). Other less predictable natural events are volcanic eruptions, sink holes, earthquakes, and mudslides.

4. Vulnerability analysis

- identifies vulnerabilities for which threat events exist. The goal is to identify applicable vulnerabilities (flaws or weaknesses) that can be exploited by the potential threat (identified earlier).

5. Risk identification

Risks should be identified as early as possible. A best practice for risk identification is by using a structured brainstorming session that draws on the experience of the project team.

6. Risk analysis

During risk analysis, the sources of the risks are revisited, followed by an estimate of the likelihood of occurrence. The last step in risk analysis is to identify existing mechanisms that control the risk, followed by an assessment of the strengths and weaknesses of the system.

7. Risk treatment

Based on the gap analysis results and the risk assessment, appropriate and justified options, or controls for treating risks will be identified, selected, and documented in a risk treatment plan.

The following are some of the options for the treatment of risks:

1. Avoid risk
2. Reduce likelihood of occurrence
3. Reduce the consequences
4. Transfer risk
5. Accept risk

8. Risk monitoring.

Monitoring risk ensures all controls are monitored at a frequency commensurate with their significance to the organization.

Integration with Other Management Practices

Risk management can be linked to four other areas of management practice.

1. **Budgeting**. Risk management addresses the need to mitigate identified risks. The treatment plan or actions require time and resources; therefore, a link to the budgeting process is useful.
2. **Business planning**. The organization should develop business planning that is aligned to the organization's objectives.
3. **Internal audit.** Organizations should use information from information assurance risk management to contribute to the organization's internal audit and internal control reviews.
4. **Periodic reporting**. A periodic report is a tool that the management can use to monitor key risks.

LEARNING CONTENTS (Information Assurance Policy)

Policy is a formal rule of conduct, controlled by some authority. The information assurance policy is undoubtedly the most important element for a successful information assurance management program.

Importance of Policy

1. To establish a foundation for an effective information assurance management program.
2. To establish and define appropriate security conduct.
3. To support regulatory and governance requirements and fiduciary duties.
4. To ensure consistent implementation of security controls.
5. To support the coordination of activities of internal and external groups.

Policy and Other Governance Functions

Policies provide direction to an organization's intents and objectives that meet its requirements in various areas. Guidelines and procedures are developed and aligned to these policies. They are distributed to the employees to create awareness and better understanding of the organization's processes. This ensures effective implementation of them.

Policy Development Steps

The policy development steps start from gathering key reference materials, defining a framework for policies, developing a policy, and reviewing and approving the policy, as well as the enforcement processes.

1. Information Gathering

- Information gathering is essential to policy development. This ensures that developed policies are consistent with the organization's culture, vision, and mission.

2. Policy Framework Definition

- compile a list containing the topics covered. Organizations may want to prioritize policy coverage

based on the urgency of issues to be addressed. The organization should define how it intends to present the information assurance policies. It may be useful for the organization to identify the target audience group that the policy will address.

3. **Policy development**
   - The message should be kept brief, with words such as shall (imperative form) applied to indicate that an item in a policy statement is mandatory and such words should be used consistently throughout the policy. Standards, procedures, and guidelines may be referenced in the policies.

4. **Review and Approval**
   - Several review cycles are recommended to gain support from the key players. As more feedback is received, the policy has greater chances to be accepted later. At a minimum, it should be a three-step process peer review; review by internal parties such as internal audit, IT, human resources, or legal department; and finally, review by senior management. The final step in the review process is endorsement by senior management.

5. **Enforcement**
   - Policy enforcement is the final crucial step to ensure the success of an organization's information assurance management program. Suitable actions should be taken to detect and respond to noncompliance. It is appropriate to discuss noncompliance issues with all parties involved and the human resource department.

Policy Layout

The actual layout of a policy document varies from organization to organization. However, a policy document should consider the following components as a starting point:

a. **Objectives** - define the goals of the policy and the issues to be addressed.

b. **Scope** - establishes which resources of the organization are covered by the policy. This can include all electronically stored, processed, transmitted, printed, faxed, or verbal information.

c. **Definitions** - define important terms and definitions to be used throughout the policy document to establish a common ground of understanding among all readers.

d. **Responsibilities** - establish who is responsible for the review, maintenance, and implementation of the policy.

e. **Compliance** - detail the consequences if the policy is violated.

f. **References** - list materials referred to in the policy document such as specific regulations, decrees, mandates, standards, and other policies.

g. **Related documents** - list relevant documents that are created in relation to the policy document.

h. **Effective date** - specify the effective date of the policy.

i. **Signature** - document should have a signature of approval by senior management.

SUMMARY

- The three key components of information assurance are people, process, and technology.
- The three types of structure of an information assurance organization are centralized structure,

distributed structure, and hybrid structure.

- ❖ Assets are tangible or intangible. The different types of assets are data/information, hardware, intangible, people, service, and software.
- ❖ The risk management process includes background planning, asset analysis, threat analysis, vulnerability analysis, risk identification, risk analysis, risk treatment, and risk monitoring.

REFERENCES

Information Assurance Handbook: Effective Computer Security and Risk Management Strategies, Corey Schou & Steven Hernandez McGraw Hill Education, 2016, ISBN-13: 978-0-07-182631-0

Information assurance: managing organizational IT security risks. Joseph George Boyce, Dan Wesley Jennings. Butterworth–Heinemann is an imprint of Elsevier Science.2002

E-SOURCES:

https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l21/lec.html