STUDY GUIDE FOR MODULE NO. 1

Unit 1 – Information Assurance Basics

MODULE OVERVIEW

This part provides key concepts, vital components, and definitions, fundamental to integrating effective information assurance. It focuses on the development of an information assurance strategy based on the size and complexity of the organization and at the same time discusses the importance and drivers of information assurance, such as why information assurance is important, fundamental principles in information assurance, and the consequence of failure. It also explains the requirements in information assurance and defines the key elements of risks. Last part emphasizes the need to ensure that the implementation of information assurance is done.

MODULE LEARNING OBJECTIVES

At the end of this, students are expected to:

1. Define information assurance.
2. Discuss the importance, fundamental principles, and consequence of failure of information assurance
3. Define the key elements of risks in information assurance.
4. Understand the information assurance management system and the plan-do-check-implementation model.
5. Explain the common laws, regulations, standards, and other guidelines in the global enterprise.

LEARNING CONTENTS (Information Assurance)

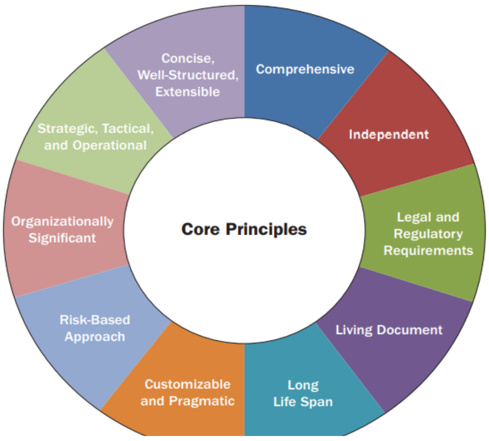
What is Information Assurance (IA)?

IA is the process for protecting and defending information by ensuring its confidentiality, integrity, and availability. At its most fundamental level, IA involves protecting the rights of people and organizations. There are two perspectives to consider.

1. IA can provide organizations with the ability to protect their own rights as entities to survive, coexist, and grow, since information is so integral to their management and operations.
2. IA can provide organizations with the ability to protect the rights of other parties that support and interact with them.

LEARNING CONTENTS (Developing an Information Assurance Strategy)

The information assurance strategy is based on ten core principles. These principles fulfill the information assurance requirements and objectives of most organizations. The size, complexity, and organizational environment will drive the relative importance of each of the principles.


Core Principles
Comprehensive
Independent
Legal and Regulatory Requirements
Living Document
Long Life Span
Customizable and Pragmatic
Risk-Based Approach
Organizationally Significant
Strategic, Tactical, and Operational
Concise, Well-Structured, Extensible

Ten Core Principles

1. **Comprehensive** An organization's information assurance strategy and resulting policies and programs should cover topics, areas, and domains needed for modern organizations. Each topic, domain, and area

within a policy should contain sufficient breadth and detail to support strategic, tactical, and operational implementation.

2. **Independent** An organization's information assurance strategy should contain independent contents and perspectives related to the defined mission. Organizations are various sizes and use products and services from vendors. To be useful for a heterogeneous community, an organization's information assurance strategy should provide a neutral view of information assurance. Constituent parts within organizations should identify their assurance needs and develop tactical and operational controls in accordance with the strategic plan. Organizations must be cautious not to specify mechanisms, products, or procedural steps to attain organizational information assurance objectives at a strategic level. That level of detail is best left at the tactical and operational level. Organizations should consider vendor-independent strategies while incorporating vendor-specific information into tactical and operational plans.
3. **Legal and Regulatory Requirements.** An organization's information assurance strategy must be consistent with existing laws and regulations applicable to but not limited to information assurance, human resources, healthcare, finance, disclosure, internal control, and privacy within the organizational context. Organizations should refer to existing legal frameworks and regulations in their information assurance strategies, so leaders understand how to fulfill the regulatory requirements of their industry or environment.
4. **Living Document.** An organization's information assurance strategy should be written as a living document comprised of independent components. In smaller organizations with little employee turnover, culture may sustain practices. However, organizations benefit from updated written policies, procedures guidance, and standards to direct operations. Organizations should use the ideas, concepts, and approach outlined in this work to keep their own policies, procedures, standards, and practices up to date.
5. **Long Life Span** Although information assurance is a dynamic, fast-moving, and rapid-changing discipline, it requires a stable strategic foundation. To increase the value and relevance of an organization's information assurance strategy, the strategy must focus on the fundamentals of information assurance that remain constant over time. This is supported by tactical and operational components.
6. **Customizable and Pragmatic** Organizations should develop a flexible information assurance strategy. The strategy should be applicable to a broad spectrum of organization functions independent of size and should consider varied objectives and infrastructure complexity. Organizations should adopt and adapt their tactical and operational plans to reflect identified organizational information assurance requirements and risk profiles. The suggested controls provided throughout this work can serve as guidance.
7. **Risk-Based Approach** In a risk-based approach, organizations identify their risk profiles and prioritize them. Since each organization has a unique risk profile, it must select controls appropriate to its risk tolerance. An organization's information assurance strategy must be broad enough to give guidance to sub-components with diverse risk profiles. This is analogous to risk portfolio approaches in finance. Risk tolerance and profiles are explained later in this work.
8. **Organizationally Significant** Information assurance should be considered significant in an organization's strategy and ongoing operations, and it is a significant investment and area of concern for any organization. Information assurance is part of an organization just like basic accounting. For example, if organizations choose to ignore accounting, they will be subject to possible fines and issues with shareholders, but more

importantly, they will be subject to fraud and internal control issues. Information assurance provides controls for an organization's most important assets while bringing visibility into operational and strategic risk.

9. **Strategic, Tactical, and Operational** The organization's information assurance strategy provides a framework to assist senior managers and executives in making strategic (long-term) planning and decisions. It provides information to aid in tactical (midterm) planning and decisions for managers. In addition, an organization's information assurance strategy contains information useful to employees and line managers who make operational (short-term) planning and decisions.
10. **Concise, Well-Structured, and Extensible** Ideally, an organization's information assurance strategy addresses wide-ranging information assurance topics, organized systematically. To help maximize benefits, the structure of a strategy document should facilitate the easy retrieval and use by readers. The structure and contents of the organization's information assurance strategy should demonstrate high cohesion and low coupling. Each topic should be discussed to the appropriate level completely on its own (high cohesion), and its contents should not be highly dependent (low coupling) on other topics. This approach makes the policy extensible by enabling the easy addition of new information (topics) and by providing a modular approach to information assurance for the user.

LEARNING CONTENTS (The Need for Information Assurance)

The information assets and infrastructure of organizations are constantly threatened. The dynamic threat environment has increased the need for information assurance. Information assurance is not just a technology issue but is a business and social issue as well. Ultimately, the goal of information assurance is to protect the information and infrastructure that supports the mission and vision of an organization through compliance to regulations, risk management, and organizational policies.

Information assurance consists of protecting information and services against disclosure, transfer, modification, or destruction (either intentional or unintentional) and ensuring the availability of information in a timely manner. Information assurance also considers the authentication used in a system and how strongly actions can be repudiated. Basically, it ensures only the approved entities receive the accurate information they require when they need it. Securing information by implementing suitable and cost-effective controls ensures critical and sensitive information assets are protected adequately.

Protection of Critical and Sensitive Assets

It is a sound business practice to require that critical and sensitive assets be protected. Prior to implementing security controls, an organization must identify the critical business processes and value of the associated assets. The interdependencies between different business processes should be understood for a precise model of the prioritized security control to be implemented.

Compliance to Regulations and Circulars/Laws

Compliance to regulations ensures organizational sustainability. Each day there are new regulatory compliance requirements. Organizations operating in multiple economies or regulatory environments require extra effort to analyze regulatory urgency. Whether requirements stem from international or local laws and regulations, the organization is required to analyze how the requirements can be addressed without compromising the policies and procedures already available within the organization. Understanding how the relevant regulations and standards are in line with one another is the foundation of an effective, efficient, and sustainable compliance. From a governmental perspective in addition to guidelines and laws, some governments have “enforcement controls” required for public- or private-sector organizations. Examples of these would be general circulars, advisories, and directives.

Meeting Audit and Compliance Requirements

From an information assurance point of view, **auditing** is a process that checks and verifies compliance with generally accepted standards, a particular regulation, or a specific requirement. In addition, an audit ensures compliance efforts meet established organizational objectives and follow agreed-upon risk management controls. These different considerations lead to a common goal of compliance through meeting one or more audit requirements and regulations. Ideally, auditors work with intimate knowledge of the organization to understand the resources subject to audit. Security audits are part of the continuous process of establishing and maintaining practical policies; they are not just something to “put up with.” An audit is a sampling process applicable generally to the entire organization. Among other things, a good audit should review the effectiveness of the organization’s security policies and practices. A complete audit provides a report on the areas of noncompliance and nonconformity regarding the effectiveness of that policy within the context of the organization’s objectives, structure, and activities.

Providing Competitive Advantage

Frequently, individuals fail to recognize that information assurance is a competitive advantage. However, it becomes obvious in the case of a bank. Would you choose to put assets into a bank if it had an inadequate information system? Organizations with proactive controls stay competitive and survive longer. Further, the use of personally identifiable information and personal finance information is now considered commonplace in almost any organization. Breeches of this information not only can be costly from a financial perspective but can also damage an organization’s goodwill or public perception. Viewing information assurance as a differentiator may not be as clear-cut in other markets. For example, one may argue information assurance has no place in a social networking site. However, a social networking site that leaks pictures, message board posts, and user information to the wrong audience will quickly lose its users and therefore possibly its greatest asset (marketing information about its users). Maintaining a competitive advantage means remaining responsive to current or potential challenges. Successful organizations and those that achieve consistent milestones that exceed the average for its industry have a competitive advantage. A company with strong information assurance practices can build a trusted brand that enhances its business proposition. There are typically two identified types of competitive advantage. They are cost advantage and differentiation advantage. A competitive advantage exists when the organization can give the same benefits as competitors at a lower cost (cost advantage) or to give benefits that outdo those of competing products (differentiation advantage). Having a competitive advantage enables the organization to create value for its customers and make a profit or succeed in its mission. Organizations with strong information assurance are differentiated from their competition as noted in the prior examples of the bank and social media site.

LEARNING CONTENTS (Information Assurance Principles)

The seven principles specify that information assurance should do the following:

1) Be a business enabler
2) Protect the interconnecting element of an organization's systems
3) Be cost effective and cost beneficial
4) Establish responsibilities and accountability
5) Require a robust method
6) Be assessed periodically
7) Be restricted by social obligations

Information Assurance: Business Enabler

Information assurance is a business enabler and a competitive advantage rather than an obstacle. It allows the organization to achieve its intended objectives. The imposition of disruptive rules and procedures comes from a lack of understanding of business requirements. Frequently, these rules and procedures unnecessarily disrupt normal business operations. Through the implementation and operation of suitable controls, information assurance assists in achieving the organization's vision and mission by protecting its critical assets and resources. Prior to implementation, organizations should identify which controls are to be implemented and weigh the pros and cons associated with each. Security rules or procedures used to protect vital assets while simultaneously supporting the organization's overall vision and mission should be a goal of every senior manager or executive. When information assurance is properly implemented, it ensures business confidence and competitive advantage; therefore, assurance should be a primary agenda and not a hindrance or an afterthought. Situations exist where a decision may be made not to pursue a new venture or not to adopt a new technology because it cannot be secured appropriately because of unacceptable risk. An example is wireless networking. Some financial organizations have banned the use of IEEE 802.11 (Wi-Fi) networks until enhanced security standards for these networks become available. Thus, information assurance may act as an essential barrier to prevent the adoption of unsafe business practices, rather than as an enabler for business. However, a bank developing a secure mobile application for banking may increase customer satisfaction, reduce personnel costs, and gain customers because of convenience differentiation.

Information Assurance: Protects the Fabric of an Organization's Systems

Information systems provide the interconnecting elements of effective management of organizations. If, however, the information system does not demonstrate the security elements of the MSR model, management cannot make informed decisions. Effective protection from threats requires not only information systems but also information assurance to be an interconnecting, essential part of the entire management system. Security efforts are not silo efforts; they are the essential binding fiber. Information assurance is a shared responsibility and involves not only the IT organization and other employees. Information assurance should be incorporated into the current management strategy system and requires participation from all functional units. Any information assurance protection program should take into consideration the people, processes, and technology aspects from the MSR model. If one does not do this, the organization will be unable to garner the required support and will not meet its business objectives effectively. Information assurance involves constant review, monitoring, and improvement based on the risk decisions made by management.

Information Assurance: Cost Effective and Cost Beneficial

Information has varying value based on its criticality and sensitivity. Therefore, the protection requirements should be proportional to the value of the information/assets protected and the associated risk. A thorough analysis of the costs and benefits of information assurance may examine either quantitative or qualitative aspects to ensure investment on controls meet expectations. Security investments should take into consideration the cost of designing, implementing, and maintaining the controls; the values of information assets; the degree of dependency on the information systems; and the potential risk and impact the organization is likely to face. Investing in information assurance is both a horizontal and vertical effort. Information assurance is also a crosscutting program. All information systems and services of an organization have an information assurance requirement. Therefore, an investment should be made in every project for information assurance. This can be thought of as a variable cost. The more services, projects, and information the organization chooses to process, store, or transmit, the greater the information assurance requirements will be. There is also a fixed-cost aspect to information assurance, which is often the “vertical” aspect of information assurance. Organizations need to have an information assurance program firmly established. This function of an organization is the anchor for the horizontal security efforts and the management area of information assurance for the organization. From this function, common controls and cost-effective security are designed, implemented, and monitored.

Information Assurance: Shared Responsibilities

System owners, including cloud or outsourced service providers, should share information about planned and implemented security controls so that users can be aware of current efforts and know that the relevant systems are sufficiently secure. Identified critical systems should meet a predefined baseline acceptance level of security. System owners should remember to inform their business users or clients about security controls selected, the nature of the controls implemented, and why the controls are necessary. Peter Drucker’s 1968 book The Age of Discontinuity reminds us that knowledge work knows no hierarchy. In addition, information itself knows no individual or organizational boundaries. Information is available to those who need it. As an information assurance corollary, information can be secured adequately only when all who have access follow established procedures. Thus, information assurance is a team effort that transcends the IT function. The assignment of responsibilities may be to internal or external parties. Clearly defined security responsibilities (both individual and functional level) encourage best practices by users. Refer to Chapter 9 for detailed information assurance roles and responsibilities.

Information Assurance: Robust Approach

Information assurance requires a complete and integrated approach that considers a wide range of processes. This comprehensive approach extends throughout the entire information life cycle. Security controls operate more effectively in concert with the proper functioning of other business process controls. Interdependencies within an information system exist by definition; therefore, a thorough study should be performed before a determination of compatibility and feasibility of controls is made.

Information Assurance: Reassessed Periodically

Information systems and the environments in which they operate are always evolving. Security requirements change rapidly in parallel with emerging technologies, threats, and vulnerabilities. Therefore, there are always new risks. Changing from a centralized to a decentralized IT environment and the increasing amount of information processed in a complex environment make operations challenging and security matters an ongoing priority review. To assure controls remain relevant, an audit or review should be performed to determine the level of compliance to implemented controls. Increases in complexity or rate of change will necessitate more mature change and configuration management (CM) approaches. Organizations should continuously monitor the performance of controls by conducting regular assessments of their information systems and ensure information assurance is part of any change management and configuration management processes. This will alert management to new risks and the condition of the information systems, data, and networks that may have a negative impact on the mission of the organization.

Information Assurance: Restricted by Social Obligations

Organizations must consider social obligations in the implementation of security controls. Organizations should balance the rights and desires of the organization versus the rights of organizational employees and customers. This involves understanding the security needs of information owners and users. Expectations and policies may change concerning the suitable use of security controls. Organizations need to balance between security risks they are willing to accept versus human rights or social factors. This can lead to solving issues such as security and the workplace privacy conflict. Employee monitoring and a bring-your-own-device (BYOD) policy are areas where social obligations and information assurance often require extensive analysis.

Implications from Lack of Information Assurance

Despite the rise of information security incidents, organizations are still unaware of the criticality of information assurance. In general, you must apply both due care and due diligence to ensure a system is operating within acceptable social and legal norms.

a. **Due care** is the development and implementation of policies and procedures to aid in performing the ongoing maintenance necessary to keep an information assurance process operating properly to protect assets and people from threats. Systems must be working in accordance with the expectations of a reasonable person in a situation. Due care prevents negligence.

b. **Due diligence** is the reasonable investigation, research, and understanding of the risks an organization faces before committing to a particular course of action. The organization should do its homework and ensure ongoing monitoring.

Penalties from a Legal/Regulatory Authorities

In the wake of countless corporate scandals and acts of negligence, regulations and laws exist to ensure internal controls are implemented to protect the interests of the public and stakeholders.

Common themes from various legal/regulatory authorities are

a. Abuse Hacking, theft, password sharing
b. Critical infrastructure protection Finance and banking, natural resources, power, water, food, logistics, and military
c. Intellectual property Copyright, patent, and trademark
d. Privacy Personal information

In safeguarding the respect and good reputation of the organization, it is vital that personnel and business partners follow best-practice information assurance actions to reduce the probability of something bad happening to critical information. All partners share, in common, a risk assumed by one partner. The following are some of the issues that affect corporate reputations that are addressed through effective and periodic information assurance training or awareness programs:

- Employee misconduct
- Customer complaints
- Security incidents and breaches

LEARNING CONTENTS (Information Assurance Concepts)

When dealing with information assurance and its subcomponent information security, you should be familiar with three primary security objectives—confidentiality, integrity, and availability—to identify problems and provide proper solutions.

1. Confidentiality

Confidentiality and privacy are related terms but are not synonymous. Confidentiality is the assurance of data secrecy where no one can read data except for the intended entity. Confidentiality should prevail no matter what the data state is—whether data resides on a system, is being transmitted, or is in a particular location (for example, a file cabinet, a desk drawer, or a safe). Privacy, on the other hand, involves personal autonomy and control of information about oneself. Both are discussed in this chapter. The word classification merely means categorization in certain industries. Assign an appropriate sensitivity categorization to information to maintain confidentiality. Different categorizations will address the degree of security controls needed. For example, a range of military classification (categorization in the military) includes unclassified, confidential, secret, and top secret. A military document classified (categorized) as top secret will require control mechanisms to eliminate threats that may expose the location or characteristics of an important asset.

2. Integrity

People understand integrity in terms of dealing with people. People understand the sentiment “Jill is a woman of integrity” to mean Jill is a person who is truthful, is trustworthy, and can be relied upon to perform as she promises. When considering integrity in an information assurance perspective, organizations will use it not only from a personnel perspective but also from a systems perspective. In information systems, integrity is a service that assures that the information in a system has not been altered except by authorized individuals and processes. It provides assurance of the accuracy of the data and that it has not been corrupted or modified improperly. Integrity may be achieved by applying a mathematical technique whereby the information will later be verified. Examples of integrity controls are watermarks, bar codes, hashing, checksums, and cyclic redundancy check (CRC). A second form of integrity control manages the processes to enter and manipulate information. For example, a physician (and the patient) would want the integrity of medical records. The records should reflect the actual data from the laboratory, and once the data is stored, it should be stored so it is unchangeable outside defined processes.

3. Availability

Availability is the service that assures data and resources are accessible to authorized subjects or personnel when required. The second component of the availability service is that resources such as systems and networks should provide sufficient capacity to perform in a predictable and acceptable manner. Secure and quick recovery from disruptions is crucial to avoid delays or decreased productivity. Therefore, it is necessary that protection mechanisms should be in place to ensure availability and to protect against internal and external threats. Availability is also often viewed as a property of an information system or service. Most service level agreements and measures of performance for service providers surround availability above all else. The availability of a system may be one of its most marketable properties.

These concepts relate to providing assurances and trust surrounding the actions of an individual or a system proactively and reactively.

1. **Nonrepudiation.** Digital transactions are prone to frauds in which participants in the transaction could repudiate (deny) a transaction. A digital signature is evidence that the information originated with the asserted sender of the information and prevents subsequent denial of sending the message. Digital signatures may provide evidence that the receiver has in fact received the message and that the receiver will not be able to deny this reception. This is commonly known as nonrepudiation. The term nonrepudiation describes the service that ensures entities are honest in their actions. There are variants of nonrepudiation, but the most often used are as follows:

   • Nonrepudiation of source prevents an author from false refusal of ownership to a created or sent message, or the service will prove it otherwise.

   • Nonrepudiation of acceptance prevents the receiver from denying having received a message, or else the service will prove it otherwise.

2. **Identification, Authentication, Authorization, and Accountability.** Identification, authentication, authorization, and accountability are the essential functions in providing an access management system. The overall architecture of an access management system includes the means of identifying its users, authenticating a user's identity and credentials, and setting and controlling the access level of a user's authorization. In addition, it should provide for logging and auditing the trail of a user's activity in search of privilege violations or attempted violations and accounting for system resource usage.

   The current industry practice for implementing IAAA security is identity management. Identity management includes, as its first step, the use of logon IDs and passwords. The system verifies that the password entered by a user matches the password linked with the individual's logon ID. A policy should state that the password needs to be changed frequently and must have a minimum strength. Strong passwords must not be guessed easily, such as a mother's maiden name or place of birth, and they must have a combination of characters, symbols, and numbers to increase security. Bear in mind the current threat environment almost renders passwords useless unless combined with other controls or factors to increase the strength of authentication.

Steps of IAAA

1. Identification (User Declares Who They Are)

Identification is a method for a user within a system to introduce oneself. In an organizationwide identification requirement, you must address identification issues. An example would be more than one person having the same name. Identifiers must be unique so that a user can be accurately identified across the organization. Each user should have a unique identifier, even if performing multiple roles within the organization. This simplifies matters for users as well as the management of an information system. It also eases control in that an organization may have a centralized directory or repository for better user management. A standard interface is crucial for ease of verification process. The same goes for the availability of the verification process itself. This is to ensure that access can be granted only with verification.

2. Authentication (User Proves Who They Are)

This validates the identification provided by a user. In other words, it makes sure the entity presenting the identification can further prove to be who they claim. To be authenticated, the entity must produce minimally a second credential. Three basic factors of authentication are available to all types of identities.

- What you should know (a shared secret, such as a password, which both the user and the authenticator know)
- What you should have (a physical identification, such as a smartcard, hardware token, or identification card)
- What you are (a measurable attribute, such as biometrics, a thumbprint, or facial recognition)

3. Authorization (Determine and Grant Access to the System)

Once a user presents a second credential and is identified, the system checks an access control matrix to determine their associated privileges. If the system allows the user access, the user is authorized.

4. Accountability (System Access Granted, Actions Logged & Audited)

The act of being responsible for actions taken within a system is accountability. The only way to ensure accountability is to identify the user of a system and record their actions. Accountability makes nonrepudiation extremely important.

Assets, Threats, Vulnerabilities, Risks, and Controls

Asset is anything valuable to the organization. An information asset, if compromised, may cause losses should it be disclosed, be altered, or become unavailable. An information asset can be tangible or intangible, such as hardware, software, data, services, and people. The losses can also be tangible or intangible, such as the number of machines or a smeared reputation.

Threats are potential events that may cause the loss of an information asset. A threat may be natural, deliberate, or accidental.

Vulnerabilities are weaknesses exploited by threats. Examples of vulnerabilities include software bugs, open ports, poorly trained personnel, and outdated policy.

Risk expresses the chance of something happening because of a threat successfully exploiting a vulnerability that will eventually affect the organization. Examples of impact are loss of competitive edge, loss of confidential information, systems unavailability, failure to meet a service level agreement, and tarnished reputation. The probability of a particular risk occurring is known as **likelihood**. To manage risks, controls are established.

Controls are protective measures or mechanisms that reduce risks. The types and likelihood of threats vary based on the nature of the business, location, and time.

Common Threats

- Threats originate with humans, technology, and environmental conditions. Examples are human errors when entering information, misconfigured systems, malicious software, and natural disasters such as floods and earthquakes. When these threats exist and the associated vulnerabilities are not controlled, information could be lost, become unavailable, or become corrupt, hence compromising information assurance. Threats can be divided into four categories: a. ***force majeure***, b. ***deliberate acts***, c. ***human failure***, and d. ***technical failure***. The following are the common threats found in a typical IT environment.

1. Errors and Negligence
2. Fraudulent and Theft Activities
3. Loss of Infrastructure
4. Malware
5. Attackers
6. Employee Sabotage
7. Industrial Espionage
8. Invasion of Privacy
9. Phishing and Spear Phishing
10. Spamming
11. Vulnerabilities

Controls

- Controls are actions taken or mechanisms established to resolve information assurance issues. Controls to protect identified assets vary from one organization to another because they depend on issues such as an organization's objectives, availability of resources, and risk profiles.
- The implementation of controls is driven by the following factors:
  - To protect critical and sensitive information assets
  - To ensure compliance with regulatory and legislation requirement
  - To gain competitive edge
  - To mitigate risks and avoid unnecessary operational, financial, and customer losses

Categories of Controls

- **Management** controls are security controls that are strategic and suitable for planning and monitoring purposes. Examples of controls in this category are the information assurance policy and information assurance risk management exercises.
- **Operational** controls are controls used in day-to-day operations to ensure the secure execution

of business activities. Examples of controls in this category are mechanisms or tools for IT support and operations, physical and environmental security controls, and information security incident-handling processes and procedures.

- **Technical** controls are the possible technical and physical implementation of information assurance solutions and recommendations. Examples of controls in this category are access controls, as well as security audit and monitoring tools.

Key considerations to be made when implementing a control

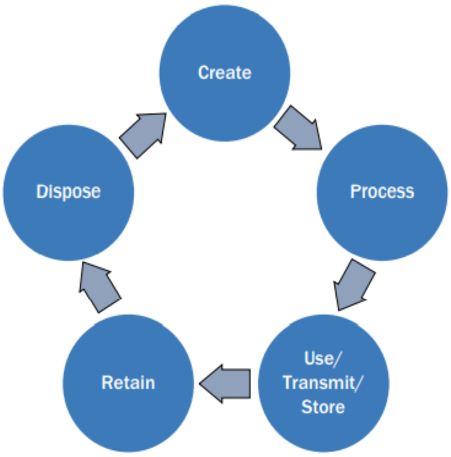
1. Establish Balance Between Managing Risk and Implementing Controls
2. Ensure the Proper Controls Are Selected and Implemented
3. Assess and Review Controls

LEARNING CONTENTS (Information Assurance Management System)

To manage information assurance effectively and efficiently, there is a need to establish a system. This system is the information assurance management system (IAMS). The IAMS combines the components of people, process, and technology, and it is based on a sound risk management approach to protecting information assets. It stresses the importance of a process-based approach in managing and improving information assurance.

Security Considerations for the Information Asset Life Cycle

Information has life cycles. The term information life cycle means the cyclical stages through which information flows, typically characterized as creation, processing, use or transmission, storage, retention, and eventually disposal. Organizations constantly acquire data from their environment as well as create information internally. Both data and information are processed and used to meet organizational goals and objectives. The result is stored for retrieval and later use. Information may be archived and retained as part of legal requirements.



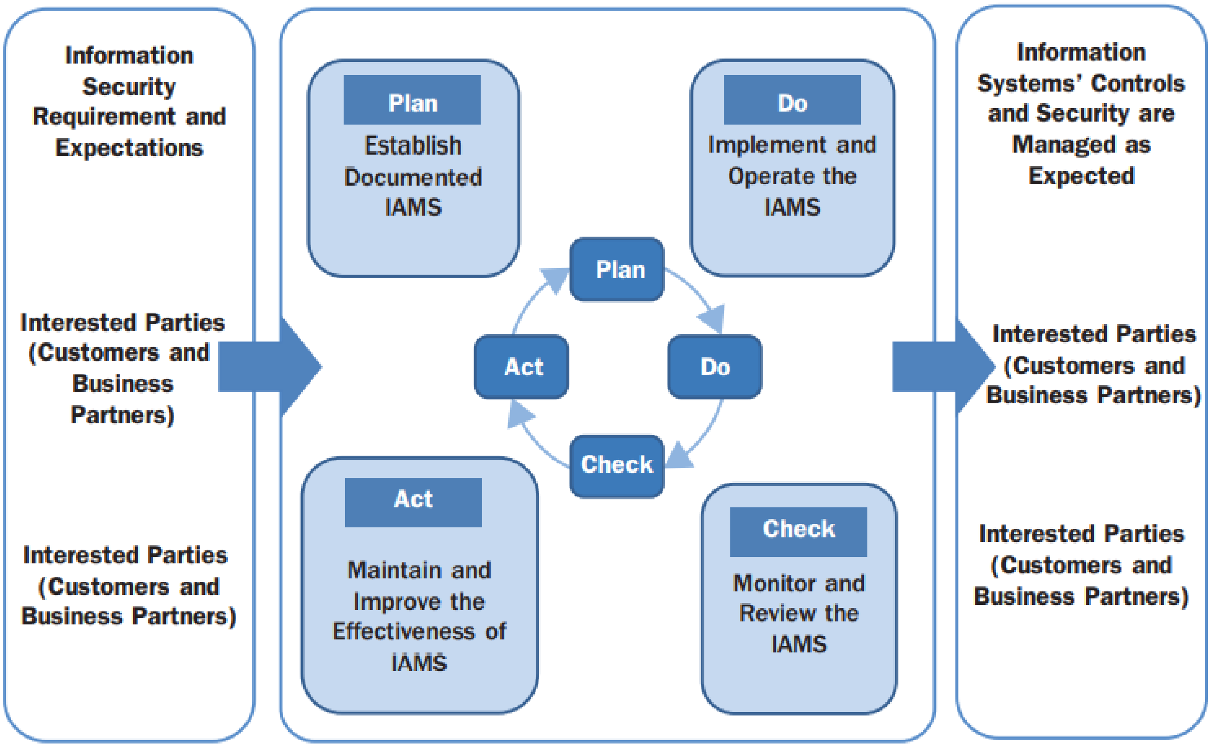
Information Life Cycle Model

Plan-Do-Check-Act Model

The Plan-Do-Check-Act model demonstrates the process of managing security throughout the life cycle. This includes the implementation of a continuous improvement process to attain an effective information assurance management system. The IAMS is adaptable to future changes and developments, business objectives, requirements, and processes; in addition, it reflects the needs of customers, suppliers, and business partners.

The outcome of each PDCA cycle is a managed information assurance environment in the organization.

• Plan	-	Establish the IAMS.
• Do	-	Implement, operate, and maintain the IAMS.
• Check	-	Monitor and review the IAMS.
• Act	-	Execute, maintain, and improve the IAMS.


Information Security Requirement and Expectations
Interested Parties (Customers and Business Partners)
Interested Parties (Customers and Business Partners)
Plan
Establish Documented IAMS
Do
Implement and Operate the IAMS
Plan
Act
Do
Check
Act
Maintain and Improve the Effectiveness of IAMS
Check
Monitor and Review the IAMS
Information Systems' Controls and Security are Managed as Expected
Interested Parties (Customers and Business Partners)
Interested Parties (Customers and Business Partners)

PDCA model applied to IAMS process

LEARNING CONTENTS (Current Practices, Regulations and Plans)

Due Care and Due Diligence
The concepts of due care and due diligence are often discussed when evaluating the need for appropriate information assurance controls and risk management.

Due Care
Due care can be defined as the responsibility that managers and their organizations have a duty to provide for information assurance to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed.

Due Diligence
Due diligence is the continuous activities an organization takes to ensure the efforts established in due care are effective and operating as intended.

Specific Laws and Regulations
It is important to understand the relevant legislation and regulations applicable to the organization. They form an important part of the security requirements for establishing protection strategies. They encourage the organization to establish policies and procedures ensuring compliance

Intellectual Property Law
The importance of intellectual property law to the profession of information assurance is obvious since it is directly related to ideas or information. It is concerned with how a company protects what it owns and describes remedies if this law is violated. The protection of intellectual property depends on the type of resource protected. Even where the laws in specific countries are different, understanding the terminology is important. Examples

of intellectual property are as follows:

- **Patents**

A patent grants legal ownership of an invention to an individual or organization. • The inventor applies formally for a patent, after which ownership, development, and use of the design is limited to the patent holder for a specific period. • A patent holder may grant a license to others to use the design information typically for a certain amount.

- **Trademarks**

A trademark is any distinguishing name, symbol, logo, sound, or character that establishes identity for an organization, product, or service. • A trademark can be registered and filed in the appropriate jurisdiction.

- **Trade secrets**

A trade secret is proprietary information important for its owner's economic survival and profitability. It requires special skill, ingenuity, expense, and effort to develop and defend proprietary information. Owners of trade secrets should take reasonable steps to protect the information.

- **Copyrights**

A copyright protects the expression of ideas as opposed to the protection of ideas (as for patents). It does not require the author to file for copyright protection because the law comes into effect as soon as the idea is expressed in a tangible form.

Privacy Laws

The principles addressed in privacy and data protection laws of many economies have these four items in common:

- The collection of data should be by lawful means and with the consent of the owner or by the authorized regulatory body. Organizations must always check with existing laws if such activity is allowed or not.
- Data should be accurate, complete, and kept up to date.
- Data should be reasonably protected from possible security breaches.
- Individuals have the right to make corrections to data and to make necessary amendments.

SUMMARY

- Information Assurance is the process for protecting and defending information by ensuring its confidentiality, integrity, and availability.
- The information assurance strategy is based on ten core principles: comprehensive, independent, legal and regulatory requirements, living document, long life span, customizable and pragmatic, risk-based approach, organizationally significant, strategic, tactical, and operational, and concise, well-structured, and extensible
- The seven principles specify that information assurance should do the following: (1) Be a business enabler; (2) Protect the interconnecting element of an organization's systems; (3) Be cost effective and cost beneficial; (4) Establish responsibilities and accountability; (5) Require a robust method; (6) Be assessed periodically; and (7) Be restricted by social obligations.

- To ensure a system is operating within acceptable social and legal norms, apply due care and due diligence.
- Common themes from various legal/regulatory authorities are (1) Abuse Hacking, theft, password sharing (2) Critical infrastructure protection Finance and banking, natural resources, power, water, food, logistics, and military (3) Intellectual property Copyright, patent, and trademark and (4) Privacy Personal information.
- Three primary security objectives—confidentiality, integrity, and availability.
- Steps of IAAA are (1) Identification (User Declares Who They Are); (2) Authentication (User Proves Who They Are); (3) Authorization (Determine and Grant Access to the System); and (4) Accountability (System Access Granted, Actions Logged & Audited).
- Common threats in a typical IT environment are Errors and Negligence; Fraudulent and Theft Activities; Loss of Infrastructure; Malware; Attackers; Employee Sabotage; Industrial Espionage; Invasion of Privacy; Phishing and Spear Phishing; Spamming; and Vulnerabilities.
- Information has life cycles. Organizations constantly acquire data from their environment as well as **create** information internally. Both data and information are **process**ed and **use**d to meet organizational goals and objectives. The result is **store**d for retrieval and later use. Information may be archived and **retain**ed as part of legal requirements. Finally, when the organization has no use for it, the information is **dispose**d.

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.snia.org/sites/default/education/tutorials/2009/spring/security/EricHibbard-Introduction-Information-Assurance.pdf

https://www.itgovernanceusa.com/information/information-assurance

https://www.scribd.com/document/310608707/Information-Assurance-Plan