# Information Systems Security [ INSY3073 ]

## **PART I:** Chapters **1** to **4**


Prepared by:

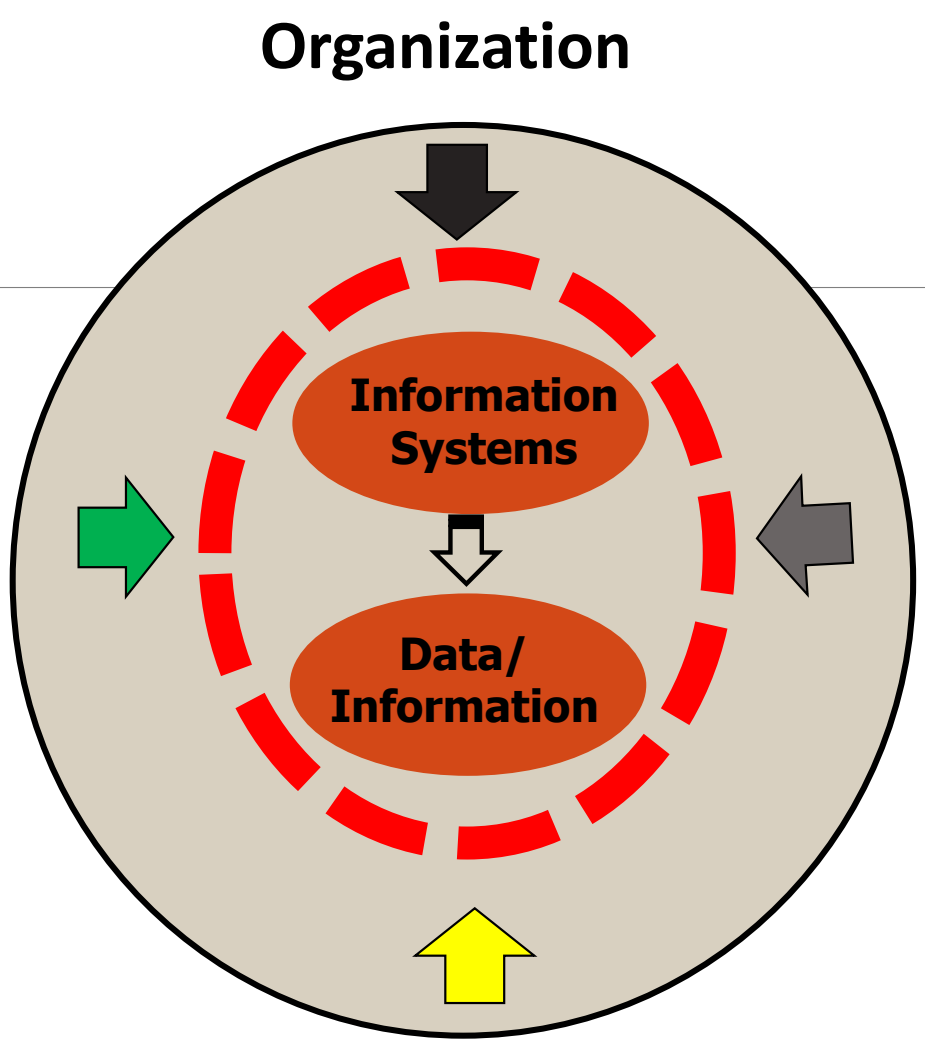
**Lemma Lessa (PhD)**

*Associate Professor* of Information Systems
School of Information Science
Addis Ababa University


**FEBRUARY 2025**

SCAN ME

SCAN ME




## Information Systems Security

# Introduction

## Security

- A state of being secure and free from danger or harm.
- The actions taken to make someone or something secure.

# *Introduction . . .*

## ❑ Information Security

- Protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology.

# Introduction . . .

- Every organization, whether public or private and regardless of size, has information it wants to protect.
  - It could be customer information, product or service information, and/or employee information.
  - Regardless of the source, it is the organization's job to protect the information to the best of its ability.

# Introduction . . .

- The history of information security begins with the concept of computer security.
- In the early days of computers, computer security was about the protection of the physical location and assets associated with computers from outside threats, but it later came to represent all actions taken to protect information systems from losses.

# Course Description

- The course provides a beginner-level understanding of information security principles, technologies, and practices.
- It explores the fundamental principles of information security within the context of organizations.

# Learning Outcomes

- Define key concepts related to information security.
- Describe common security technologies such as firewalls, intrusion detection/prevention systems, and encryption.
- Describe the principles of security risk management in the context of information security.

# Learning Outcomes

- Comprehend legal and ethical issues related to information security.
- Recognize the implications of privacy laws and regulations.
- Stay updated on emerging threats and vulnerabilities in the cybersecurity landscape.

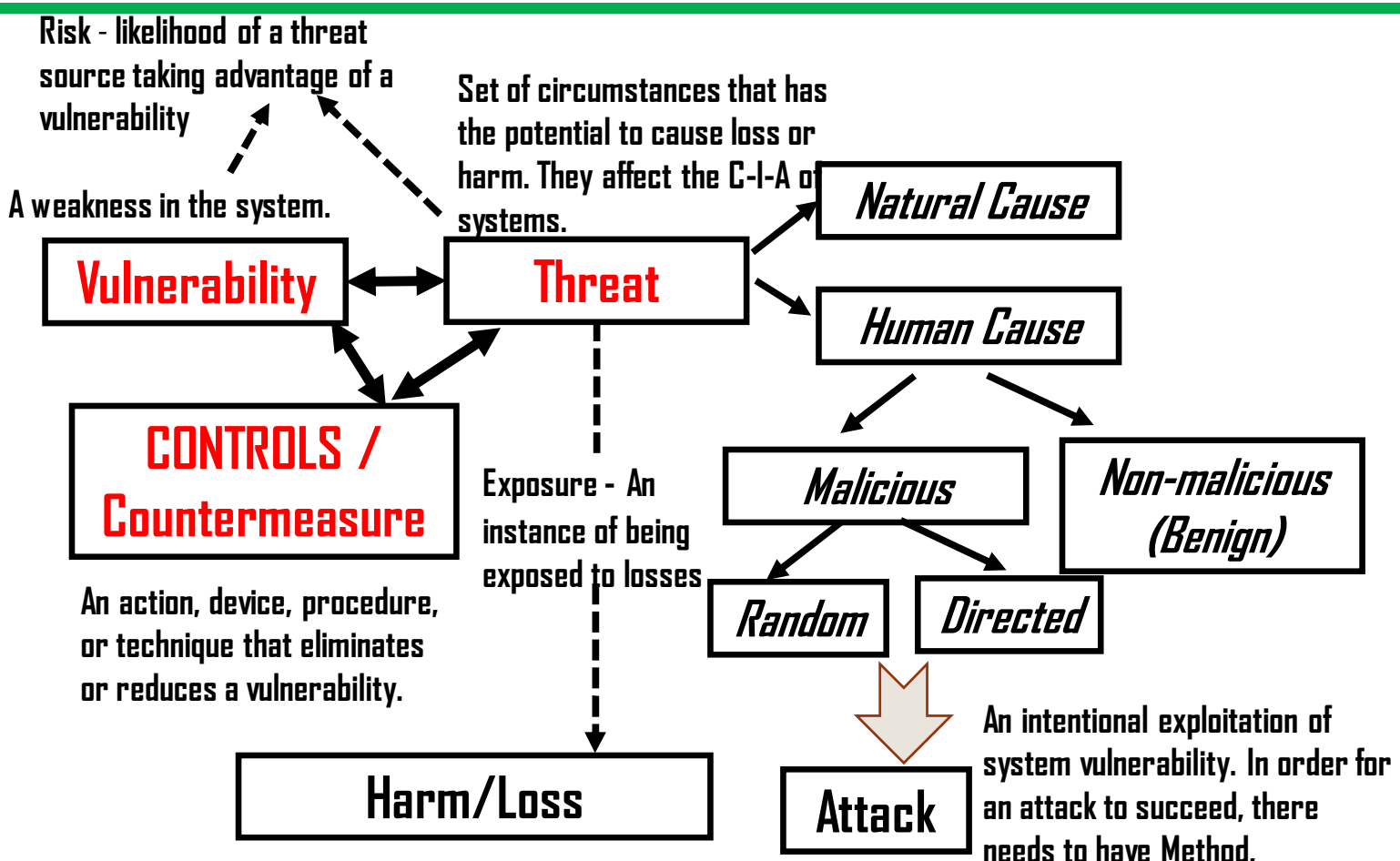
| Course Content | | |
|---|---|---|
| **Topic (Chapters)** | Duration (Week) | Reading list |
| **Chapter 1: Introduction to Information Security**<br>1.1. Definition of Information Security<br>1.2. History of Information Security<br>1.3. The Need for Information Security<br>1.4. Key Information Security Concepts<br>1.5. Security and organizations<br>1.6. Balancing Information Security and Access<br>1.7. Approaches to Information Security Implementation<br>1.8. Information Security Threats and Attacks | 2 weeks | Ref (1): Module 1 & 2 |
| **Chapter 2: Information Security Management**<br>2.1. Management of Information Security<br>2.2. Information Security Planning and Governance<br>2.3. Information Security Policy, Standards, and Practices<br>2.4. Security Education, Training, and Awareness Program<br>2.5. Information Security Blueprint, Models, and Frameworks | 2 weeks | Ref (1): Module 3 |

| | | |
|---|---|---|
| **Chapter 3: Risk Management**<br>3.1. Introduction to Risk Management<br>3.2. The Risk Management Process<br>3.3. Risk Treatment/Risk Response | 2 weeks | Ref (1): Module 4 |
| **Chapter 4: Contingency Planning**<br>4.1. Introduction to Contingency Planning<br>4.2. Fundamentals Of Contingency Planning<br>4.3. Incident Response<br>4.4. Disaster Recovery<br>4.5. Business Continuity | 2 weeks | Ref (1): Module 5 |
| **Chapter 5: Legal, Ethical, and Professional Issues in Information Security**<br>5.1. Law and Ethics in Information Security<br>5.2. International Laws and Legal Bodies<br>5.3. Ethics And Information Security | 2 weeks | Ref (1): Module 6 |

| | | |
|---|---|---|
| **Chapter 6: Security and Personnel**<br>6.1. Security and Personnel<br>6.2. Positioning The Security Function<br>6.3. Staffing The Information Security Function<br>6.4. Employment Policies and Practices<br>6.5. Personnel Control Strategies | 2 weeks | Ref (1): Module 7 |
| **Chapter 7: Security Tools/Technologies**<br>7.1. Intrusion Detection and Prevention Systems<br>7.2. Firewall Technologies<br>7.3. Protecting Remote Connections<br>7.4. Intrusion Detection and Prevention Systems<br>7.5. Scanning and Analysis Tools<br>7.6. Introduction to Cryptography<br>7.7. Encryption Methods | 2 weeks | Ref (1): Module 8,9,10 |
| **Chapter 8: Implementing Information Security**<br>8.1. Introduction to Information Security Implementation<br>8.2. The Systems Development Life Cycle<br>8.3. Information Security Project Management<br>8.4. Technical Aspects of Implementation<br>8.5. Nontechnical Aspects of Implementation<br>8.6. Information Security Maintenance | 2 weeks | Ref (1): Module 11 |

| | | |
|---|---|---|
| **Assessment Criteria** | The evaluation shall be based on both formative and summative assessments which include: | |
| | **Assessment Forms** | **% of credit allotted** |
| | • Test 1<br>• Test 2<br>• Participation and Attendance<br>• Assignment<br>• Final examination | 20<br>20<br>10<br>10<br>40 |

| | |
|---|---|
| **Reference (Main Text and Possible Reading lists)** | **Main Text**<br><br>1. Whitman, M.E. & Mattord, H.J. (2022) Principles of Information Security, Seventh Edition, Cengage Learning Inc., Australia.<br>**Reading lists**<br><br>2. Rhodes-Ousley, M. (2013) Information Security: The Complete Reference; McGraw Hill Education, New York.<br>3. Whitman, M.E. & Mattord, H.J. Management of Information Security, Fourth Edition, Course Technology, 2014.<br>4. Stallings, William and Lawrie Brown. Computer Security Principles and Practice (4th ed). New York: Pearson Education Ltd., 2015. |




Refers to the negative consequences of an actualized threat. Happens once vulnerability is exploited. Can be reduced or eliminated by protecting ourselves against threats. Harmful acts – Four ways (Interception, Interruption, modification, Fabrication) – these acts affect C-I-A of systems.

# Information Systems Security

## [ INSY 3073 ]

# Chapter 1: Introduction to Information Security


Compiled by:

**Lemma Lessa (PhD)**

*Associate Professor* of Information Systems
School of Information Science
Addis Ababa University



FEBRUARY 2025

# Key Information Security Concepts

# Key concepts

- **Asset** - The organizational resource that is being protected.
  - An asset can be logical, such as a Web site, software information, or data
  - An asset can be physical, such as a person, computer system, hardware, or other tangible object.
  - Assets, particularly information assets, are the focus of what security efforts are attempting to protect.

# Key concepts …

- **Access** - A subject or object's ability to use, manipulate, modify, or affect another subject or object.
  - Authorized users have legal access to a system
  - Hackers must gain illegal access to a system.
  - Access controls regulate this ability.

# Key concepts …

- **Attack** - An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.
  - Attacks can be active or passive, intentional or unintentional, and direct or indirect.
    - Someone who casually reads sensitive information not intended for his or her use is committing a passive attack.
    - A hacker attempting to break into an information system is an intentional attack. A lightning strike that causes a building fire is an unintentional attack.
    - A direct attack is perpetrated by a hacker using a PC to break into a system. An indirect attack is a hacker compromising a system and using it to attack other systems.

# Key concepts …

- **Control, safeguard, or countermeasure** - Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve security within an organization.

- **Exploit** - A technique used to compromise a system.
  - Threat agents may attempt to exploit a system or other information asset by using it illegally for their gain.

# Key concepts …

- **Exposure** - A condition or state of being exposed
  - In information security, exposure exists when a vulnerability is known to an attacker.
- **Loss** - A single instance of an information asset suffering damage or destruction, unintended or unauthorized modification or disclosure, or denial of use.
  - When an organization's information is stolen, it has suffered a loss.

# Key concepts …

- **Protection profile or security posture** - The entire set of controls and safeguards - including policy, education, training and awareness, and technology - that the organization implements to protect the asset.
  - The terms are sometimes used interchangeably with the term security program, although a security program often comprises managerial aspects of security, including planning, personnel, and subordinate programs.

# Key concepts …

- **Risk** - The probability of an unwanted occurrence, such as an adverse event or loss.
  - Organizations must minimize risk to match their risk appetite - the quantity and nature of risk they are willing to accept.
- **Subjects and objects of attack** - A computer can be either the subject of an attack - *an agent entity used to conduct the attack* - or the object of an attack - *the target entity*.
  - A computer can also be both the subject and object of an attack. For example, it can be compromised by an attack (object) and then used to attack other systems (subject).

# Key concepts …

- **Threat source** - A category of objects, people, or other entities that represents the origin of danger to an asset - in other words, a category of threat agents (i.e., Natural and Artificial categories).
  - Threat sources are always present and can be purposeful or undirected. For example, threat agent "hackers," as part of the threat source "acts of trespass or espionage," purposely threaten unprotected information systems, while threat agent "severe storms," as part of the threat source "acts of God/acts of nature," incidentally threaten buildings and their contents.

# Key concepts …

- **Threat event** - An occurrence of an event caused by a threat agent.
  - This term is commonly used interchangeably with the term attack.
    - An example of a threat event might be damage caused by a storm.

# Key concepts …

- **Vulnerability** - A potential weakness in an asset or its defensive control system(s).
  - Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door.

# Critical Characteristics of Information (*expanded* C.I.A. triad)

# Critical Characteristics of Information

- The value of information comes from the characteristics it possesses.
- When a characteristic of information changes, the value of that information either increases or, more commonly, decreases.
- Some characteristics affect information's value to users more than others, depending on circumstances.

# Critical Characteristics of Information …

- **Confidentiality** ensures that only users with the rights, privileges, and need to access information are able to do so.
  - When unauthorized individuals or systems view information, its confidentiality is breached.
  - Confidentiality, like most characteristics of information, is interdependent with other characteristics and is closely related to the characteristic known as privacy.

# Critical Characteristics of Information …

- To protect the confidentiality of information, you can use several measures, including the following:
  - Information classification
  - Secure document storage
  - Application of general security policies
  - Education of information custodians and end users

# Critical Characteristics of Information …

- **Integrity** - Information has integrity when it is in its expected state and can be trusted.
  - The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state.

# Critical Characteristics of Information …

- **Availability** - enables authorized users - people or computer systems - to access information without interference or obstruction and to receive it in the required format.

- **Accuracy** - Information has accuracy when it is free from mistakes or errors and has the value that the end user expects.
  - If information has been intentionally or unintentionally modified, it is no longer accurate.

# Critical Characteristics of Information …

- **Authenticity** - Information is authentic when it is in the same state in which it was created, placed, stored, or transferred.
- **Utility** - The utility of information is its usefulness. In other words, information has value when it can serve a purpose.
  - If information is available but is not in a meaningful format to the end user, it is not useful.

# Critical Characteristics of Information …

- **Possession** - The possession of information is the quality or state of ownership or control.
  - Information is said to be in one's possession if one obtains it, independent of format or other characteristics.
  - While a breach of confidentiality always results in a breach session, a breach of possession does not always lead to a breach of confidentiality.

# Balancing Information Security and Access

An organization can protect itself **100%** from cyber-attacks?

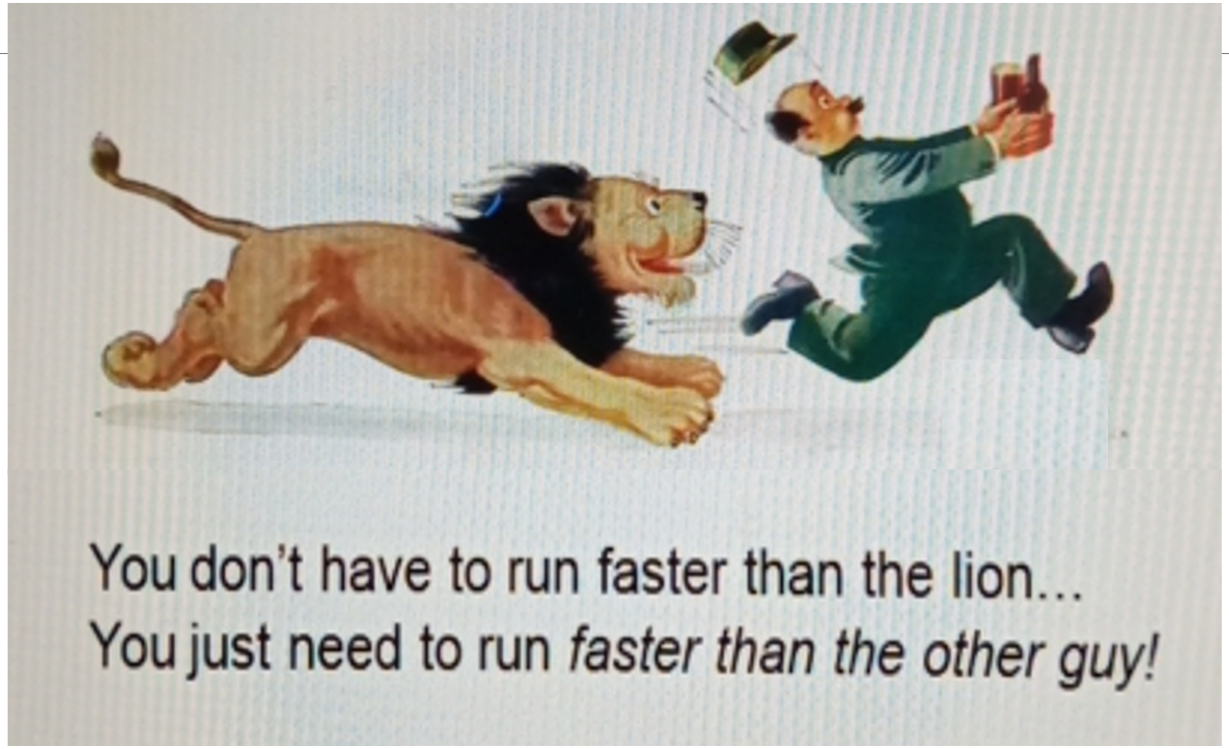
Agree / Disagree? **Why?**

# Balancing Information Security and Access

- Security begins somewhere in the organization, and cannot happen overnight.
- Securing information assets is an incremental process that requires coordination, time, and patience.

# Balancing Information Security and Access

- It takes a wide range of professionals to support a diverse information security program.
- Even with the best planning and implementation, it is impossible to obtain perfect information security. Information security cannot be absolute: It is a process, not a goal.




## Implication to InfoSec?

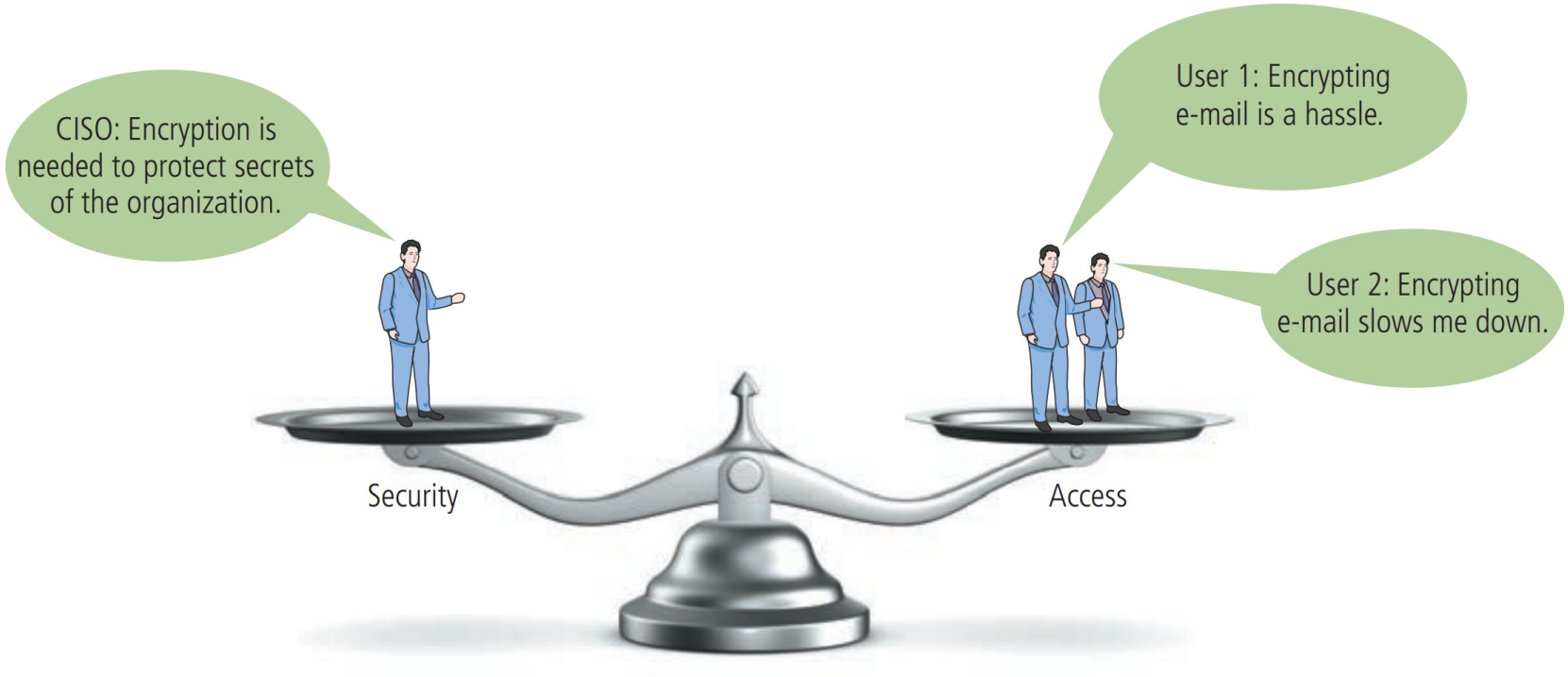
“አላህንም እመን፥
ግመልህንም እሰር።”

ነብዩ መሐመድ /ሰዐወ/

## Implication to InfoSec?

# Balancing Information Security and Access …

- You can make a system available to anyone, anywhere, anytime, through any means. However, such unrestricted access poses a danger to the security of the information.
- On the other hand, a completely secure information system would not allow anyone access.
- To achieve balance - to operate an information system that satisfies users and security professionals - the security level must allow reasonable access yet protect against threats.




Balancing information security and access

# Balancing Information Security and Access ...

- An imbalance can occur when the needs of the end user are undermined by obsessive focus on protecting and administering the information systems.

- Information security technologists and end users must recognize that both groups share the same overall goals of the organization - to ensure that data is available when, where, and how it is needed, with minimal delays or obstacles.

# Approaches to Information Security Implementation

# Approaches to Information Security Implementation

## Bottom-up approach

- A method of establishing security policies and/or practices that begins as a grassroots effort in which systems administrators attempt to improve the security of their systems.
- The key advantage of the bottom-up approach is the technical expertise of individual administrators.
- Unfortunately, the bottom-up approach seldom works because it lacks critical features such as participant support and organizational staying power.

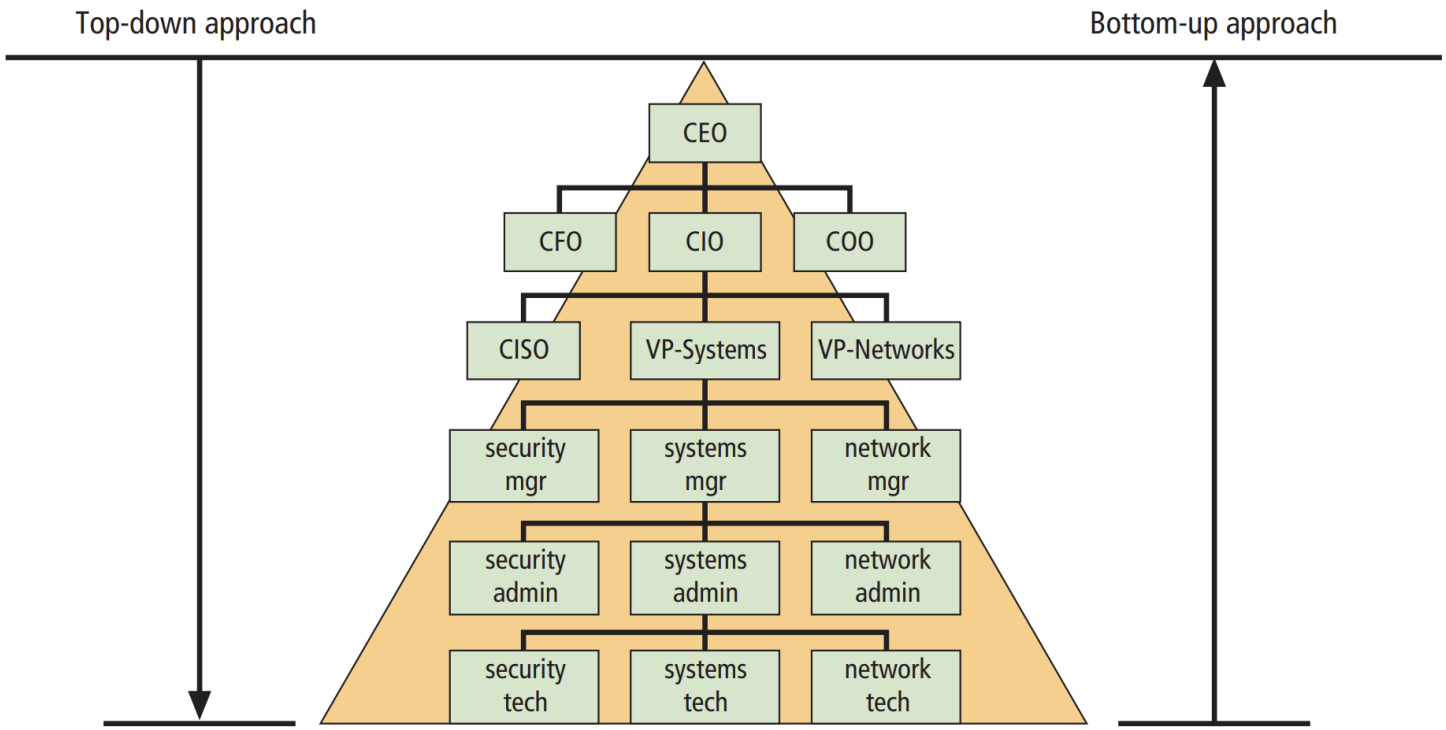
# Approaches to Information Security Implementation

## Top-down approach

- A methodology of establishing security policies and/or practices that is initiated by upper management.
- The project is formally designed and supported by upper-level managers who issue policies, procedures, and processes, dictate the goals and expected outcomes, and determine accountability for each required action.

# Approaches to Information Security Implementation

- **Top-down approach …**
  - This approach has strong upper management support, a dedicated champion, usually dedicated funding, a clear planning and implementation process, and the means of influencing organizational culture.
  - It has a higher probability of success.




Approaches to information security implementation

# Information Security Professionals

# Information Security Professionals

- Because information security is best initiated from the top down, senior management is the key component and the vital force for a successful implementation of an information security program.

- However, administrative support is also essential to developing and executing specific security policies and procedures, and of course, technical expertise is essential to implementing the details of the information security program.

# Information Security Professionals …

## ❑ Senior Management

- The senior technology officer is typically the chief information officer (CIO).
  - Other titles such as vice president of information, VP of information technology, and VP of systems may be used.

# Information Security Professionals …

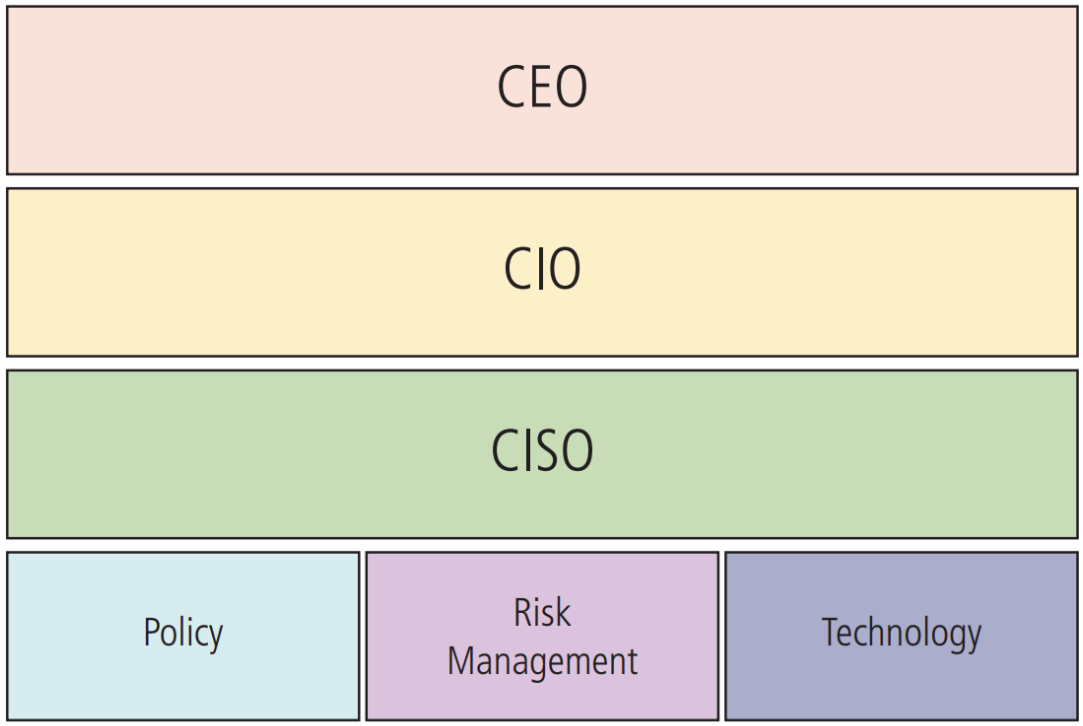
## Senior Management

- **Chief Information Officer (CIO)** - An executive-level position that oversees the organization's computing technology and strives to create efficiency in the processing and access of the organization's information.
- The CIO is primarily responsible for advising the chief executive officer, president, or company owner on strategic planning that affects the management of information in the organization.
- The CIO translates the strategic plans of the entire organization into strategic information plans for the information systems or information technology division of the organization.

# Information Security Professionals …

## ❑ Senior Management …

- **Chief Information Security Officer (CISO) -** The title typically assigned to the top information security manager in an organization.
- The CISO has primary responsibility for the assessment, management, and implementation of information security in the organization. The CISO may also be referred to as the manager for IT security, the security administrator, or by a similar title.
- The CISO usually reports directly to the CIO.




The CISO's place and roles

# Information Security Project Team

- **Champion** - A senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization
- **Team leader** - A project manager who may also be a departmental line manager or staff unit manager, and who understands project management, personnel management, and information security technical requirements
- **Security policy developers** - People who understand the organizational culture, existing policies, and requirements for developing and implementing successful policies
- **Risk assessment specialists** - People who understand financial risk assessment techniques, the value of organizational assets, and the security methods to be used

# Information Security Project Team ...

- **Security professionals** - Dedicated, trained, and well-educated specialists in all aspects of information security from both a technical and nontechnical standpoint
- **Systems administrators** - People with the primary responsibility for administering systems that house the information used by the organization
- **End users** - Those whom the new system will most directly affect. Ideally, a selection of users from various departments, levels, and degrees of technical knowledge assist the team in focusing on the application of realistic controls that do not disrupt the essential business activities they seek to safeguard.

# Information Security Threats and Attacks

# Information Security Threats and Attacks

- The primary mission of an information security program is to ensure that information assets - information and the systems that house them - are protected and thus remain safe and useful.

- The threat of attacks on information assets is a constant concern, and the need for information security grows along with the sophistication of the attacks.

# Information Security Threats and Attacks …

- When security needs and business needs collide, business wins.
  - Without the underlying business to generate revenue and use the information, the information may lose value, and there would be no need for it.
  - If the business cannot function, information security becomes less important.

# Information Security Threats and Attacks …

- Information security performs four important functions for an organization:
  - Protecting the organization's ability to function
  - Protecting the data and information the organization collects and uses, whether physical or electronic

# Information Security Threats and Attacks …

- Information security performs four important functions for an organization: …
  - Enabling the safe operation of applications running on the organization's IT systems
  - Safeguarding the organization's technology assets

# Information Security Threats and Attacks …

- The three communities of interest - general management, IT management, and information security management - are each responsible for facilitating the information security program that protects the organization's ability to function.
- Implementing information security has more to do with management than technology.
- Managing information security has more to do with risk management, policy, and its enforcement than the technology of its implementation.

# Information Security Threats and Attacks …

- To protect your organization's information, you must:

1. Know yourself - that is, be familiar with the information to be protected and the systems that store, transport, and process it

2. Know your enemy; in other words, the threats you face.

- There is wide agreement that the threat from external sources increases when an organization connects to the Internet.

# Information Security Threats and Attacks …

- To make sound decisions about information security, management must be informed about the various threats to an organization's people, applications, data, and information systems.
  - Threat agents damage or steal an organization's information or physical assets by using exploits to take advantage of vulnerabilities where controls are not present or no longer effective.
- Unlike threats, which are always present, attacks exist only when a specific act may cause a loss.

# Categories of Threats

| Category of Threat | Attack Examples |
|---|---|
| Compromises to intellectual property | Piracy, copyright infringement |
| Deviations in quality of service | Internet service provider (ISP), power, or WAN service problems |
| Espionage or trespass | Unauthorized access and/or data collection |
| Forces of nature | Fire, floods, earthquakes, lightning |
| Human error or failure | Accidents, employee mistakes |
| Information extortion | Blackmail, information disclosure |
| Sabotage or vandalism | Destruction of systems or information |
| Software attacks | Viruses, worms, macros, denial of service |
| Technical hardware failures or errors | Equipment failure |
| Technical software failures or errors | Bugs, code problems, unknown loopholes |
| Technological obsolescence | Antiquated or outdated technologies |
| Theft | Illegal confiscation of equipment or information |

# Information Security Threats and Attacks …

- Each organization must prioritize the threats it faces based on:
  - The particular security situation in which it operates
  - Its organizational strategy regarding risk, and
  - The exposure levels of its assets.

# Information Security Threats and Attacks …

## ❑ Compromises to Intellectual Property (IP)

- **IP** - Original ideas and inventions created, owned, and controlled by a particular person or organization; IP includes the representation of original ideas.
- **Software piracy -** The unauthorized duplication, installation, or distribution of copyrighted computer software, which is a violation of intellectual property.
  - The most common IP breach.

# Information Security Threats and Attacks …

## ❑ Compromises to Intellectual Property (IP) …

- IP includes trade secrets, copyrights, trademarks, and patents.
- IP is protected by copyright law and other laws, carries the expectation of proper attribution or credit to its source, and potentially requires the acquisition of permission for its use, as specified in those laws.

# Information Security Threats and Attacks …

## ❑ Deviations in Quality of Service

- An organization's information system depends on the successful operation of many interdependent support systems, including power grids, data and telecommunications networks, parts suppliers, service vendors, and even janitorial staff and garbage haulers.
- Any of these support systems can be interrupted by severe weather, intentional or accidental employee actions, or other unforeseen events.

# Information Security Threats and Attacks …

## ❑ Deviations in Quality of Service …

- **Availability disruption -** An interruption or disruption in service, usually from a service provider, which causes an adverse event within an organization.

- **service level agreement (SLA) -** A document or part of a document that specifies the expected level of service from a service provider, including provisions for minimum acceptable availability and penalties or remediation procedures for downtime.

# Information Security Threats and Attacks …

## ❑ Espionage or Trespass

- It is a well-known and broad category of electronic and human activities that can breach the confidentiality of information.
- When an unauthorized person gains access to information an organization is trying to protect.
- Attackers can use many different methods to access the information stored in an information system.

# Information Security Threats and Attacks …

## ❑ Forces of Nature

- It, sometimes called acts of God, can present some of the most dangerous threats because they usually occur with little warning and are beyond the control of people.

- These threats, which include events such as fires, floods, earthquakes, landslides, mudslides, windstorms, sandstorms, solar flares, and lightning as well as volcanic eruptions and insect infestations, can disrupt not only people's lives but the storage, transmission, and use of information.

# Information Security Threats and Attacks …

## Human Error or Failure

- This category includes acts performed without intent or malicious purpose or in ignorance by an authorized user.
- When people use information assets, mistakes happen. Similar errors happen when people fail to follow established policies.
- Inexperience, improper training, and incorrect assumptions are just a few things that can cause human error or failure.
- Regardless of the cause, even innocuous mistakes can produce extensive damage.

# Information Security Threats and Attacks …

## Information Extortion

- The act of an attacker or trusted insider who steals or interrupts access to information from a computer system and demands compensation for its return or for an agreement not to disclose the information.
- Information extortion, also known as cyber extortion, is common in the theft of credit card numbers.

# Information Security Threats and Attacks …

## Sabotage or Vandalism

- This category of threat involves the deliberate sabotage of a computer system or business or acts of vandalism to destroy an asset or damage the image of an organization.
- These acts can range from petty vandalism by employees to organized sabotage against an organization.
- Although they might not be financially devastating, attacks on the image of an organization are serious.
- Vandalism to a Web site can erode consumer confidence, diminishing an organization's sales, net worth, and reputation.

# Information Security Threats and Attacks …

## ❑ Software Attacks

- Deliberate software attacks occur when an individual or group designs and deploys software to attack a system.
- This attack can consist of specially crafted software that attackers trick users into installing on their systems.
- This software can be used to overwhelm the processing capabilities of online systems or to gain access to protected systems by hidden means.

# Information Security Threats and Attacks …

## Technical Hardware Failures or Errors

- They occur when a manufacturer distributes equipment containing a known or unknown flaw.
- These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability.

# Information Security Threats and Attacks …

## Technical Software Failures or Errors

- Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved.
- Sometimes, combinations of certain software and hardware reveal new failures that range from bugs to untested failure conditions.
- Sometimes these bugs are not errors but purposeful shortcuts left by programmers for benign or malign reasons.

# Information Security Threats and Attacks …

## Technological Obsolescence

- Antiquated or outdated infrastructure can lead to unreliable and untrustworthy systems.
- Management must recognize that when technology becomes outdated, there is a risk of losing data integrity from attacks.
- Management's strategic planning should always include an analysis of the technology currently in use.
- Ideally, proper planning by management should prevent technology from becoming obsolete, but when obsolescence is clear, management must take immediate action.

# Information Security Threats and Attacks …

## Theft

- The threat of theft is a constant.
- The value of information is diminished when it is copied without the owner's knowledge.
- Electronic theft is a more complex problem to manage and control.
  - Physical theft can be controlled easily using a wide variety of measures, from locked doors to trained security personnel and the installation of alarm systems.

# Information Security Threats and Attacks …

## Theft …

- When electronic information is stolen, the crime is not always readily apparent.
  - When someone steals a physical object, the loss is easily detected; if it has any importance at all, its absence is noted.
- If thieves are clever and cover their tracks carefully, the crime may remain undiscovered until it is too late.

# Information Systems Security

## [ INSY 3073 ]

# Chapter 2: Information Security Management


Prepared by:

**Lemma Lessa (PhD)**

*Associate Professor* of Information Systems
School of Information Science
Addis Ababa University


FEBRUARY 2025

# Management of Information Security

# Management of Information Security

- As part of the organization's management team, the InfoSec management team operates like all other management units.
- However, the InfoSec management team's goals and objectives differ from those of the IT and general management communities in that the InfoSec management team is focused on the secure operation of the organization.
- The primary focus of the **IT group** is to ensure the effective and efficient processing of information, whereas the primary focus of the **InfoSec group** is to ensure the confidentiality, integrity, and availability of information.

# Management of Information Security

- **6 P's**
  - **Planning**
  - **Policy**
  - **Programs**
  - **Protection**
  - **People**
  - **Projects**

# Management of Information Security

## [ 1 ] Planning

- Planning in InfoSec management is an extension of the broader planning in the organization.
- **InfoSec planning** - activities necessary to support the design, creation, and implementation of InfoSec strategies within the planning environments of all organizational units, including IT.
  - The IT strategy and that of the other business units provide critical information used for InfoSec planning as the CISO gets involved with the CIO and other executives to develop the strategy for the next level down.

# Management of Information Security

## [ 2 ] Policy

- Instructions that dictate certain behavior within an organization.
- Policies function like laws in an organization because they dictate acceptable and unacceptable behavior there, as well as the penalties for failure to comply.
- Policies direct how issues should be addressed and how technologies should be used.
  - Like laws, policies define what is right and wrong, the penalties for violating policy, and the appeal process.
  - Management from all communities of interest, including general staff, information technology, and information security, must make policy the basis for all information security planning, design, and deployment

# Management of Information Security

## [ 2 ] Policy …

- An organization's information security effort succeeds only when it operates in conjunction with the organization's information security policy.
- An information security program begins with policy, standards, and practices, which are the foundation for the information security program and its blueprint.
- The creation and maintenance of these elements require coordinated planning.

# Management of Information Security

- There are **three** **general InfoSec policy categories**
  - **Enterprise information security policy (EISP)** - Developed within the context of the strategic IT plan, this sets the tone for the InfoSec department and the InfoSec climate across the organization.
    - Written instructions provided by management that inform employees and others in the workplace about proper behavior regarding the use of information and information assets.
    - The CISO typically drafts the program policy, which is usually supported and signed by the CIO or the CEO.

# Management of Information Security

- There are **three** **general InfoSec policy categories …**
  - **Issue-specific security policies (ISSPs)** - These are sets of rules that define acceptable behavior within a specific organizational resource, such as e-mail or Internet usage.
  - **Systems-specific policies (SysSPs)** - A merger of technical and managerial intent, SysSPs include both the managerial guidance for the implementation of a technology as well as the technical specifications for its configuration.

# Management of Information Security

## [ 3 ] Programs

- InfoSec operations that are specifically managed as separate entities
  - An example would be a security education, training, and awareness (SETA) program or a risk management program.
    - ✓ SETA programs provide critical information to employees to maintain or improve their current levels of security knowledge.
    - ✓ Risk management programs include the identification, assessment, and control of risks to information assets.

# Management of Information Security

## [ 3 ] Programs …

- Good security programs begin and end with policy.
- Information security is primarily a management problem, not a technical one, and policy is a management tool that obliges personnel to function in a manner that preserves the security of information assets.
- Security policies are the least expensive control to execute but the most difficult to implement properly. They have the lowest cost in that their creation and dissemination require only the time and effort of the management team.

# Management of Information Security

## [ 4 ] Protection

- The protection function is executed via a set of risk management activities, as well as protection mechanisms, technologies, and tools.
  - Each of these mechanisms or safeguards represents some aspect of the management of specific controls in the overall InfoSec plan.

# Management of Information Security

## [ 5 ] People

- People are the most critical link in the InfoSec program.
- This area encompasses security personnel (the professional information security employees), the security of personnel (the protection of employees and their information), and aspects of the Security Education, Training, and Awareness (SETA) program.

# Management of Information Security

## [ 6 ] Projects

- Whether an InfoSec manager is asked to roll out a new security training program or select and implement a new firewall, it is important that the process be managed as a project.
- The final element for thoroughgoing InfoSec management is the application of a project management discipline to all elements of the InfoSec program.
- Project management involves identifying and controlling the resources applied to the project, as well as measuring progress and adjusting the process as progress is made toward the goal.

# Information Security Planning and Governance

# Information Security Planning and Governance

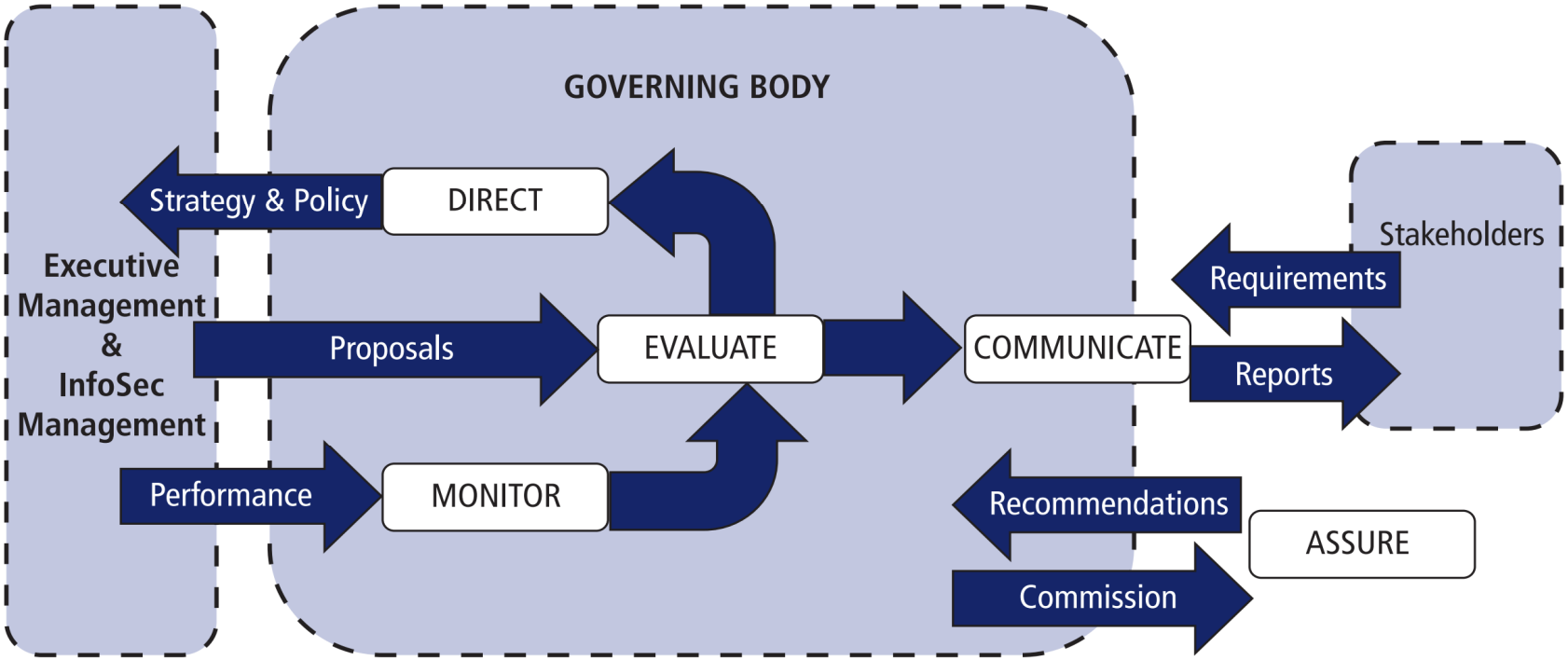
- Strategic planning sets the long-term direction to be taken by the organization and each of its component parts.
  - Strategic planning should guide organizational efforts and focus resources toward specific, clearly defined goals.
- After an organization develops a general strategy, it generates an overall strategic plan by extending that general strategy into plans for major divisions.

# Information Security Planning and Governance …

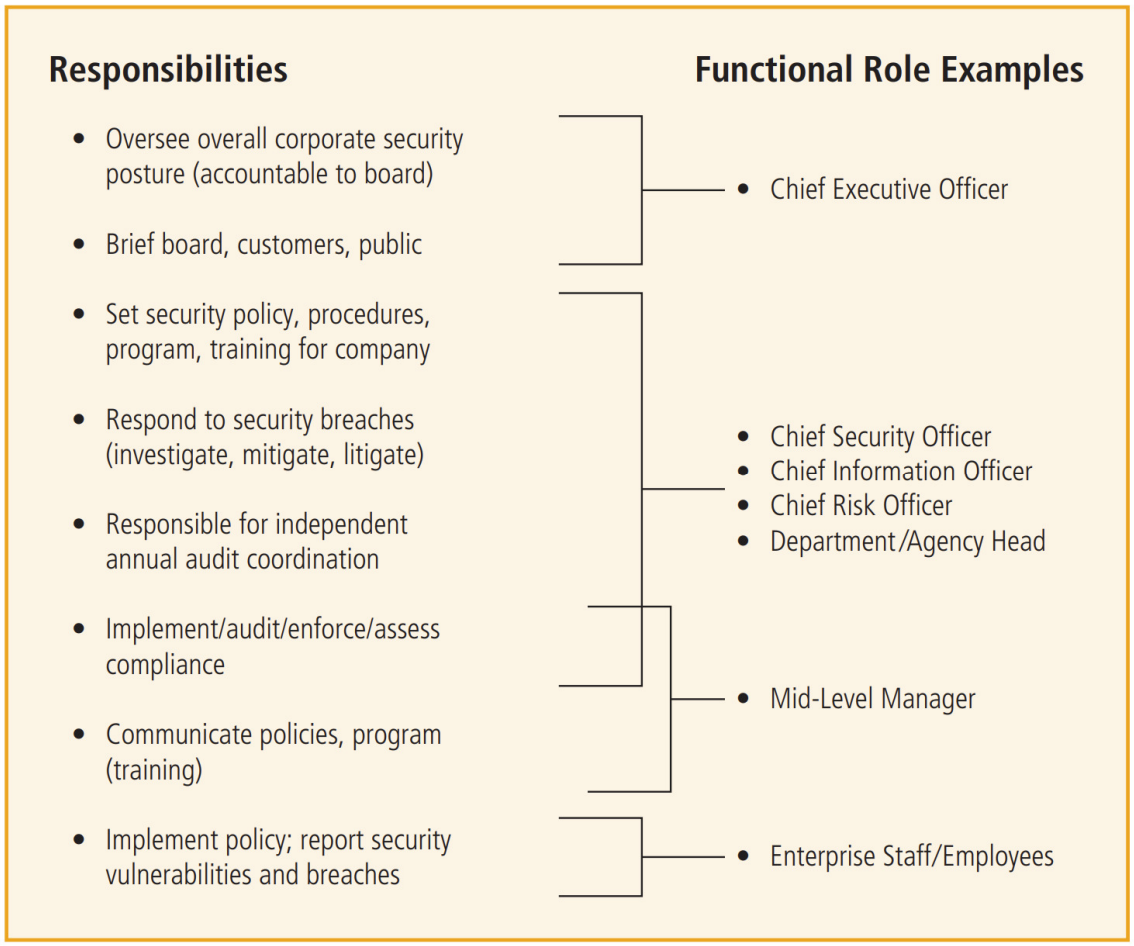
- Each level of each division then translates those plan objectives into more specific objectives for the level below.
- To execute this broad strategy, the executive team must first define individual responsibilities.
- The leadership of the information security function that delivers strategic planning and corporate responsibility is best accomplished using an approach referred to as governance, risk management, and compliance (GRC).

# Information Security Planning and Governance …

- **Information security governance** is about:
  - Strategic direction
  - Establishment of objectives
  - Measurement of progress toward those objectives
  - Verification that risk management practices are appropriate
  - Validation that the organization's assets are used properly




ISO/IEC 27014:2013 governance processes




Information security governance roles and responsibilities

# Information Security Policy, Standards, and Practices

# Information Security Policy, Standards, and Practices

- Policies do not specify the proper operation of equipment or software - this information should be placed in the standards, procedures, and practices of users' manuals and systems documentation.

- In addition, policy should never contradict law; policy must be able to stand up in court if challenged; and policy must be properly administered through dissemination and documented acceptance.
  - Otherwise, an organization leaves itself exposed to significant liability.

# Information Security Policy, Standards, and Practices

- **Standard** - A detailed statement of what must be done to comply with policy, sometimes viewed as the rules governing policy compliance.

| | |
|---|---|
| Policy | "Use strong passwords, frequently changed." |
| Standard | "The password must be at least 10 characters with at least one of each of these: uppercase letter, lowercase letter, number, and special character." |

- **Guidelines** - Nonmandatory recommendations the employee may use as a reference in complying with a policy.

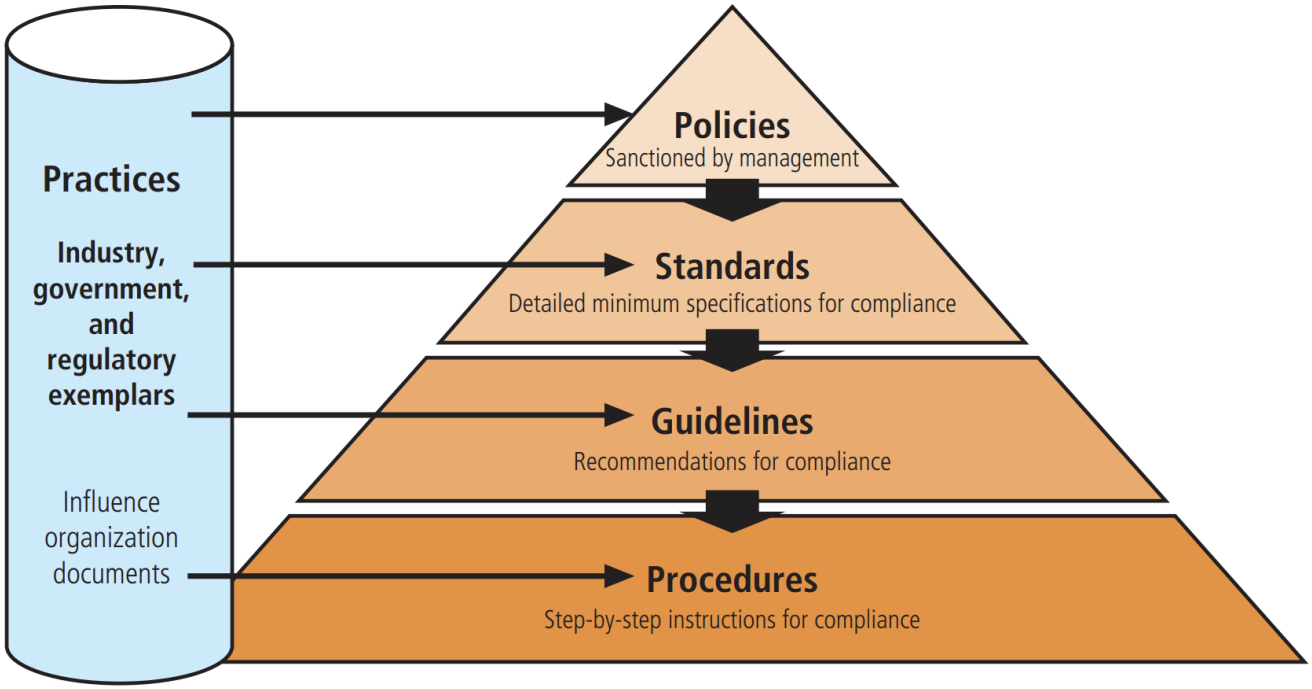
| | |
|---|---|
| Guideline | "We recommend you don't use family or pet names, or parts of your Social Security number, employee number, or phone number in your password." |

# Information Security Policy, Standards, and Practices

- **Procedures** - Step-by-step instructions designed to assist employees in following policies, standards, and guidelines.

- **Practices** - Examples of actions that illustrate compliance with policies.

| | |
|---|---|
| Practice | "According to *Passwords Today*, most organizations require employees to change passwords at least every six months." |
| Procedure | "In order to change your password, first click the Windows Start button; then ..." |




Policies, standards, guidelines, and procedures

# Information Security Education, Training, and Awareness Program

# Information Security Education, Training, and Awareness (SETA) Program

- **SETA Program** - A managerial program designed to improve the security of information assets by providing targeted knowledge, skills, and guidance for an organization's employees.
  - Once your organization has defined the policies that will guide its security program, it is time to implement a security education, training, and awareness (SETA) program.
  - The SETA program is the responsibility of the CISO and is a control measure designed to reduce incidents of accidental security breaches by employees.

# Information Security Education, Training, and Awareness (SETA) Program …

- Employee errors are among the top threats to information assets, so it is well worth developing programs to combat this threat.
  - SETA programs are designed to supplement the general education and training programs that many organizations use to educate staff about information security.
  - The SETA program consists of three distinct elements: security education, security training, and security awareness. An organization may not be able or willing to undertake all three of these elements, and it may outsource elements to local educational institutions.

# Information Security Education, Training, and Awareness (SETA) Program …

## ❑ Security Education

- Everyone in an organization needs to be trained and made aware of information security, but not everyone needs a formal degree or certificate in information security.
- When management agrees that formal education is appropriate, an employee can investigate courses in continuing education from local institutions of higher learning.

# Information Security Education, Training, and Awareness (SETA) Program …

## ❑ Security Training

- Security training provides employees with detailed information and hands-on instruction to prepare them to perform their duties securely.
- Management of information security can develop customized in-house training or outsource the training program.

# Information Security Education, Training, and Awareness (SETA) Program …

## ❑ Security Awareness

- A security awareness program is one of the least frequently implemented but most beneficial programs in an organization.
- A security awareness program is designed to keep information security at the forefront of users' minds.

# Information Security Education, Training, and Awareness (SETA) Program …

- **Security Awareness …**
  - These programs don't have to be complicated or expensive.
    - Good programs can include newsletters, security posters, videos, bulletin boards, flyers, and trinkets.
    - Trinkets can include security slogans printed on mouse pads, coffee cups, T-shirts, pens, or any object frequently used during the workday that reminds employees of security.


SETA awareness posters

| | Awareness | Training | Education |
|---|---|---|---|
| Attribute | Seeks to teach members of the organization *what* security is and what the employee should do in some situations | Seeks to train members of the organization *how* they should react and respond when threats are encountered in specified situations | Seeks to educate members of the organization as to *why* it has prepared in the way it has and why the organization reacts in the ways it does |
| Level | Offers basic *information* about threats and responses | Offers more detailed *knowledge* about detecting threats and teaches skills needed for effective reaction | Offers the background and depth of knowledge to gain *insight* into how processes are developed and enables ongoing improvement |
| Objective | Members of the organization can *recognize* threats and formulate simple responses | Members of the organization can mount effective responses using learned *skills* | Members of the organization can engage in active defense and use *understanding* of the organization's objectives to make continuous improvement |
| Teaching methods | • Media videos<br>• Newsletters<br>• Posters<br>• Informal training | • Formal training<br>• Workshops<br>• Hands-on practice | • Theoretical instruction<br>• Discussions/seminars<br>• Background reading |
| Assessment | True/false or multiple choice (identify learning) | Problem solving (apply learning) | Essay (interpret learning) |
| Impact timeframe | Short-term | Intermediate | Long-term |

# Information Security Blueprint, Models, and Frameworks

# Information Security Blueprint, Models, and Frameworks

- Once an organization has developed its information security policies and standards, the information security community can begin developing the blueprint for the information security program.

- **Information security blueprint** - In information security, a framework or security model customized to an organization, including implementation details.

  - This information security blueprint is the plan and **basis for the design, selection, and implementation of all security program elements**, including policies, risk management programs, education and training programs, technological controls, and program maintenance.

# Information Security Blueprint, Models, and Frameworks

- The organization's policy will guide the selection and development of the blueprint, and the organization will use the blueprint to guide the implementation of the rest of the security program.
  - The blueprint is the organization's detailed implementation of an information security framework.
    - The blueprint specifies tasks and the order in which they are to be accomplished, just as an architect's blueprint serves as the design template for the construction of a building.

# Information Security Blueprint, Models, and Frameworks

## Information Security framework

- It is the philosophical foundation from which the blueprint is designed, like the style or methodology in which an architect was trained.
- In information security, a specification of a model to be followed during the design, selection, and initial and ongoing implementation of all subsequent security controls, including information security policies, security education and training programs, and technological controls.

# Information Security Blueprint, Models, and Frameworks

- In choosing the framework to use for an information security blueprint, the organization should consider adapting or adopting a recognized or widely accepted information security model.

- **Information security model** - A well-recognized information security framework, usually promoted by a government agency, standards organization, or industry group.

# Information Security Blueprint, Models, and Frameworks

- Because each information security environment is unique, the security team may need to modify or adapt pieces from several frameworks.
- Experience teaches that what works well for one organization may not precisely fit another.

# Information Security Blueprint, Models, and Frameworks

- Popular information security frameworks
  - The ISO 27000 Series
  - NIST Security Models
- Many public Professional societies and private organizations promote solid best security practices.

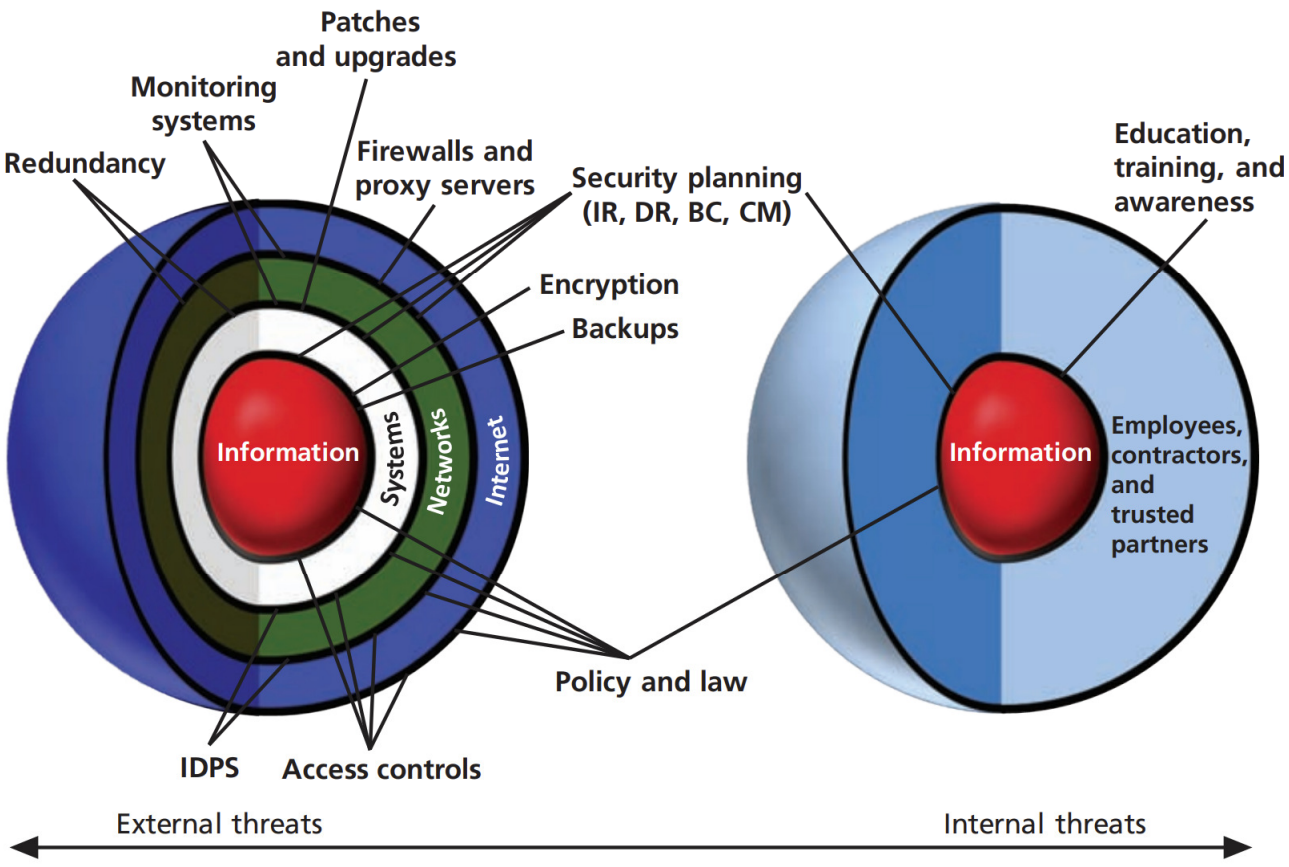
# Design of the Security Architecture

## ❑ Spheres of Security

- The spheres of security illustrate how information is under attack from a variety of sources.
- The spheres of security are the foundation of the security framework.

# Design of the Security Architecture

- Information security is **designed and implemented in three layers**: policies, people (education, training, and awareness programs), and technology. These layers are commonly referred to as **PPT**.
  - Each layer contains controls and safeguards to protect the information and information system assets that the organization values.
    - But, **before any technical controls or other safeguards can be implemented**, the policies that **define the management philosophies behind the security process** must be in place.




Spheres of security

# Design of the Security Architecture

- Information security safeguards provide three levels of control:
  - Managerial
  - Operational, and
  - Technical.

# Design of the Security Architecture

## ❑ Managerial controls

- Information security safeguards that focus on administrative planning, organizing, leading, and controlling, and that are designed by strategic planners and implemented by the organization's security administration; they include governance and risk management.

# Design of the Security Architecture

## ❑ Operational controls

- Information security safeguards focusing on lower-level planning that deals with the functionality of the organization's security; they include disaster recovery planning, incident response planning, and SETA programs.

# Design of the Security Architecture

- **Technical controls** - Information security safeguards that focus on the application of modern technologies, systems, and processes to protect information assets; they include firewalls, virtual private networks, and IDPSs.
  - While operational controls address specific operating issues, such as developing and integrating controls into the business functions, technical controls include logical access controls, such as identification, authentication, authorization, accountability (including audit trails), cryptography, and the classification of assets and users.

# Design of the Security Architecture

- **Defense in Depth** - A basic tenet of security architectures is the layered implementation of security.
- **Security Perimeter** - The boundary in the network within which an organization attempts to maintain security controls for securing information from threats from untrusted network areas.
  - The border of security that protects all internal systems from outside threats.
  - Unfortunately, the perimeter does not protect against internal attacks from employee threats or on-site physical threats.

# Information Systems Security

## [ INSY 3073 ]

# Chapter 3: Information Security Risk Management


Prepared by:

**Lemma Lessa (PhD)**

*Associate Professor* of Information Systems
School of Information Science
Addis Ababa University



FEBRUARY 2025

# Introduction to Security Risk Management

# Introduction to Security Risk Management

- **Cybersecurity risk**
  - refers to the potential harm that may result from a cyber-attack or data breach on an organization's information systems, networks, or digital assets.

# Introduction to Security Risk Management

- The upper management of an organization is responsible for overseeing, enabling, and supporting the structuring of IT and information security functions to defend its information assets.

- Part of upper management's information security governance requirement is the establishment and support of an effective risk management (RM) program.

## Introduction to Security Risk Management …

- To keep up with the competition, organizations must design and create safe environments in which their business processes and procedures can function.
- These environments must maintain confidentiality and privacy and assure the integrity of an organization's data - objectives that are met by applying the principles of risk management.

# Introduction to Security Risk Management …

- Chinese general Sun Tzu Wu's quote has direct relevance to risk management:

*If you know the enemy and know yourself, you need not fear the result of a hundred battles.*

*If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.*

*If you know neither the enemy nor yourself, you will succumb in every battle.*

## Introduction to Security Risk Management …

- **Cybersecurity Risk Management**
  - involves the process of identifying, assessing, prioritizing, and mitigating risks to an organization's digital assets and information systems.
  - The process of identifying risk, assessing its relative magnitude, and taking steps to reduce it to an acceptable level.

# Introduction to Security Risk Management …

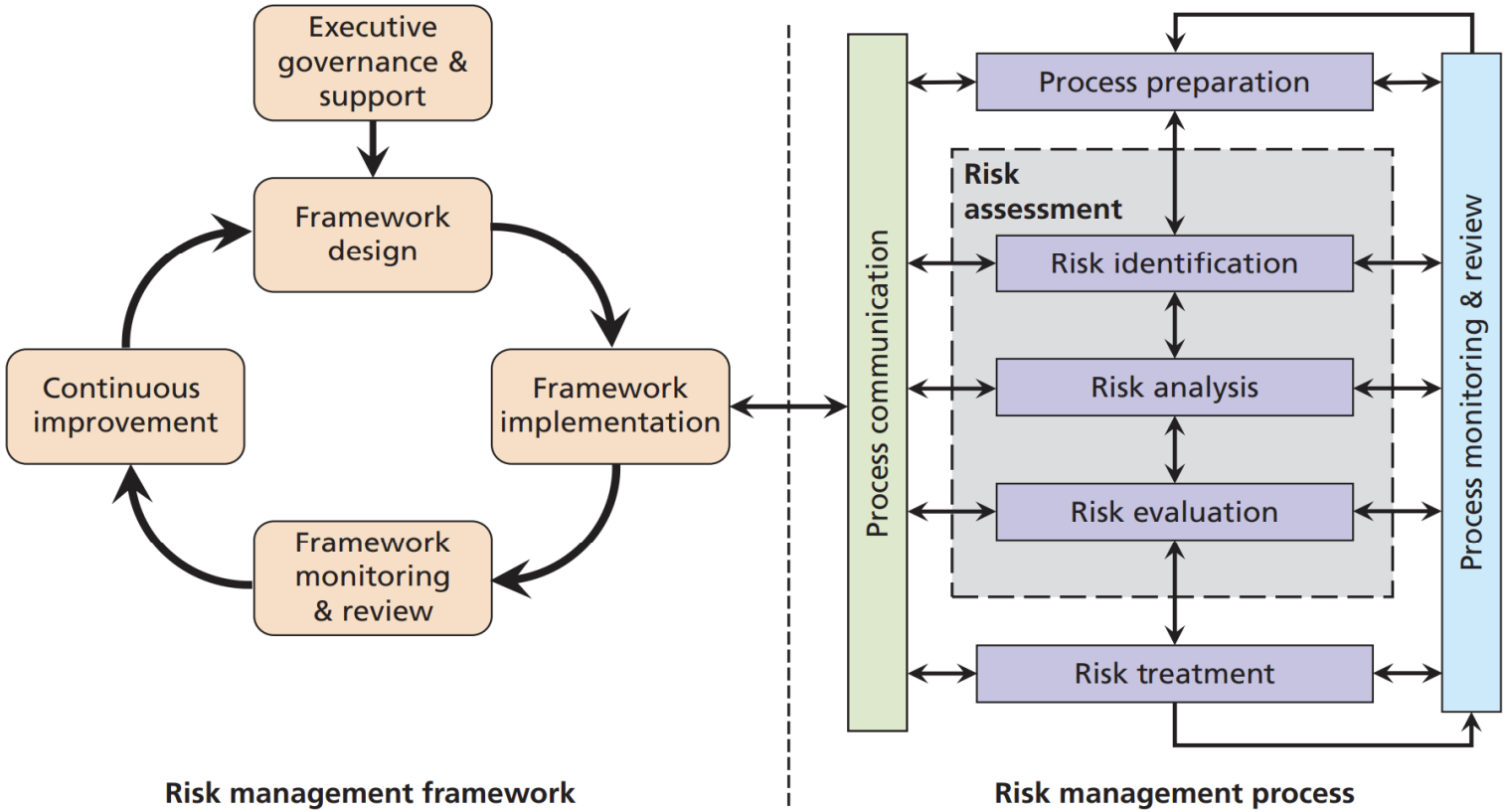
- Risk management involves discovering and understanding answers to some key questions about the risk associated with an organization's information assets:
  - Where and what is the risk (risk identification)?
  - How severe is the current level of risk (risk analysis)?
  - Is the current level of risk acceptable (risk evaluation)?
  - What do I need to do to bring the risk to an acceptable level (risk treatment)?

# Security Risk Management Process

- During the implementation phase of the RM framework, the RM plan guides the implementation of the RM process, in which risk evaluation and remediation of key assets are conducted.

- The three communities of interest must work together to address every level of risk, ranging from full-scale disasters (whether natural or human-made) to the smallest mistake made by an employee.

  - To do so, representatives from each community collaborate to be actively involved in RM process activities.




The risk management framework and process

# Security Risk Management Process …

## [ 1 ] Establishing the context

- Includes understanding both the organization's internal and external operating environments and other factors that could impact the RM process.

# Security Risk Management Process …

## [ 2 ] Identifying risk

- Creating an inventory of information assets
- Classifying and organizing those assets meaningfully
- Assigning a value to each information asset
- Identifying threats to the cataloged assets
- Pinpointing vulnerable assets by tying specific threats to specific assets

# Security Risk Management Process ...

## [ 3 ] Analyzing risk

- Determining the likelihood that vulnerable systems will be attacked by specific threats
- Assessing the relative risk facing the organization's information assets so that risk management and control activities can focus on assets that require the most urgent and immediate attention
- Calculating the risks to which assets are exposed in their current setting
- Looking in a general way at controls that might come into play for identified vulnerabilities and ways to control the risks that the assets face
- Documenting and reporting the findings of risk identification and assessment

# Security Risk Management Process ...

**[ 4 ] Evaluating the risk** to the organization's key assets and comparing identified uncontrolled risks against its risk appetite:

- Identifying individual risk tolerances for each information asset
- Combining or synthesizing these individual risk tolerances into a coherent risk appetite statement

# Security Risk Management Process …

## [ 5 ] Treating the unacceptable risk

- Determining which treatment/control strategy is best considering the value of the information asset and which control options are cost-effective
- Acquiring or installing the appropriate controls
- Overseeing processes to ensure that the controls remain effective

# Security Risk Management Process ...

- Once the project team for InfoSec development has identified the information assets with unacceptable levels of risk, the team must **choose one of four basic strategies** to treat the risks for those assets:
  - **Mitigation** - Applying controls and safeguards that eliminate or reduce the remaining uncontrolled risk
  - **Transference** - Shifting risks to other areas or to outside entities

# Security Risk Management Process ...

- **Acceptance** - Understanding the consequences of choosing to leave an information asset's vulnerability facing the current level of risk, but only after a formal evaluation and intentional acknowledgment of this decision.

- **Termination** - Removing or discontinuing the information asset from the organization's operating environment.

# Security Risk Management Process ...

## [ 6 ] Summarizing the findings

- Involves stating the conclusions of the identification, analysis, and evaluation stages of risk assessment in preparation for moving into the stage of controlling risk by exploring methods to further mitigate risk where applicable or desired.

# Summary

- Cybersecurity risk management involves identifying, assessing, and mitigating risks to an organization's information systems, data, and infrastructure.
  - It involves identifying potential cybersecurity threats and vulnerabilities, assessing the likelihood and impact of those threats, and implementing controls to mitigate or manage those risks.

# Summary …

- The goal of cybersecurity risk management is to proactively reduce the likelihood and impact of cybersecurity incidents by implementing appropriate security measures and controls.
- This process is typically ongoing and involves regular risk assessments, monitoring, and updates to security controls to adapt to changing threats and vulnerabilities.

# Information Systems Security

## [ INSY 3073 ]

# Chapter 4: Incident Response and Contingency Planning


Prepared by:

**Lemma Lessa (PhD)**

*Associate Professor* of Information Systems
School of Information Science
Addis Ababa University



FEBRUARY 2025

# Introduction to Contingency Planning

Contingency - a future event or circumstance which is possible but cannot be predicted with certainty.

# Introduction to Contingency Planning

- Because information system resources are essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption.

- Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption.

# Introduction to Contingency Planning

## Cybersecurity contingency

- A plan in place that systematically addresses how to identify, contain, and resolve any possible unexpected adverse event.
- Outlines the steps an organization will take to respond to and recover from cybersecurity incidents.

# Fundamentals of Contingency Planning

# Fundamentals of Contingency Planning

- **Contingency planning (CP)** - The overall process of preparing for unexpected adverse events.

- During CP, the IT and InfoSec communities of interest position their respective organizational units to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets, including human, information, and capital assets.

# Fundamentals of Contingency Planning …

- The main goal of CP:
  - To restore normal modes of operation with minimal cost and disruption to normal business activities after an adverse event - in other words, to make sure things get back to the way they were within a reasonable period of time.
  - Ideally, CP should ensure the continuous availability of information systems to the organization even in the face of the unexpected.

# Components of Contingency Planning ...

- **Contingency planning (CP)** - The actions taken by senior management to specify the organization's efforts and actions if an adverse event becomes an incident or disaster; CP typically includes incident response, disaster recovery, and business continuity efforts, as well as preparatory business impact analysis.

- **Contingency planning management team (CPMT)** - The group of senior managers and project members organized to conduct and lead all CP efforts.

# Components of Contingency Planning

- CP consists of **four** major components:
  - Business impact analysis (BIA)
  - Incident response plan (IR plan)
  - Disaster recovery plan (DR plan)
  - Business continuity plan (BC plan)

# Components of Contingency Planning ...

- **Adverse event** - An event with negative consequences that could threaten the organization's information assets or operations; also referred to as an incident candidate.

- **Business impact analysis (BIA)** - An investigation and assessment of adverse events that can affect the organization, conducted as a preliminary phase of the contingency planning process; it includes a determination of how critical a system or set of information is to the organization's core processes and its recovery priorities.

# Components of Contingency Planning ...

- The BIA is a preparatory activity common to both CP and risk management.
- It helps the organization determine which business functions and information systems are the most critical to the success of the organization.
- The IR plan focuses on the immediate response to an incident.

# Components of Contingency Planning ...

- Any unexpected adverse event is treated as an incident unless and until a response team deems it to be a disaster.
- Then the DR plan, which focuses on restoring operations at the primary site, is invoked.
- If operations at the primary site cannot be quickly restored - for example, when the damage is major or will affect the organization's functioning over the long term - the BC plan occurs concurrently with the DR plan, enabling the business to continue at an alternate site until the organization is able to resume operations at its primary site or select a new primary location.

# Components of Contingency Planning …

- **Incident response planning team (IRPT)**
  - The team responsible for designing and managing the IR plan by specifying the organization's preparation, reaction, and recovery from incidents.

# Components of Contingency Planning …

## ❑ Disaster recovery planning team (DRPT)

- The team responsible for designing and managing the DR plan by specifying the organization's preparation, response, and recovery from disasters, including reestablishment of business operations at the primary site after the disaster.

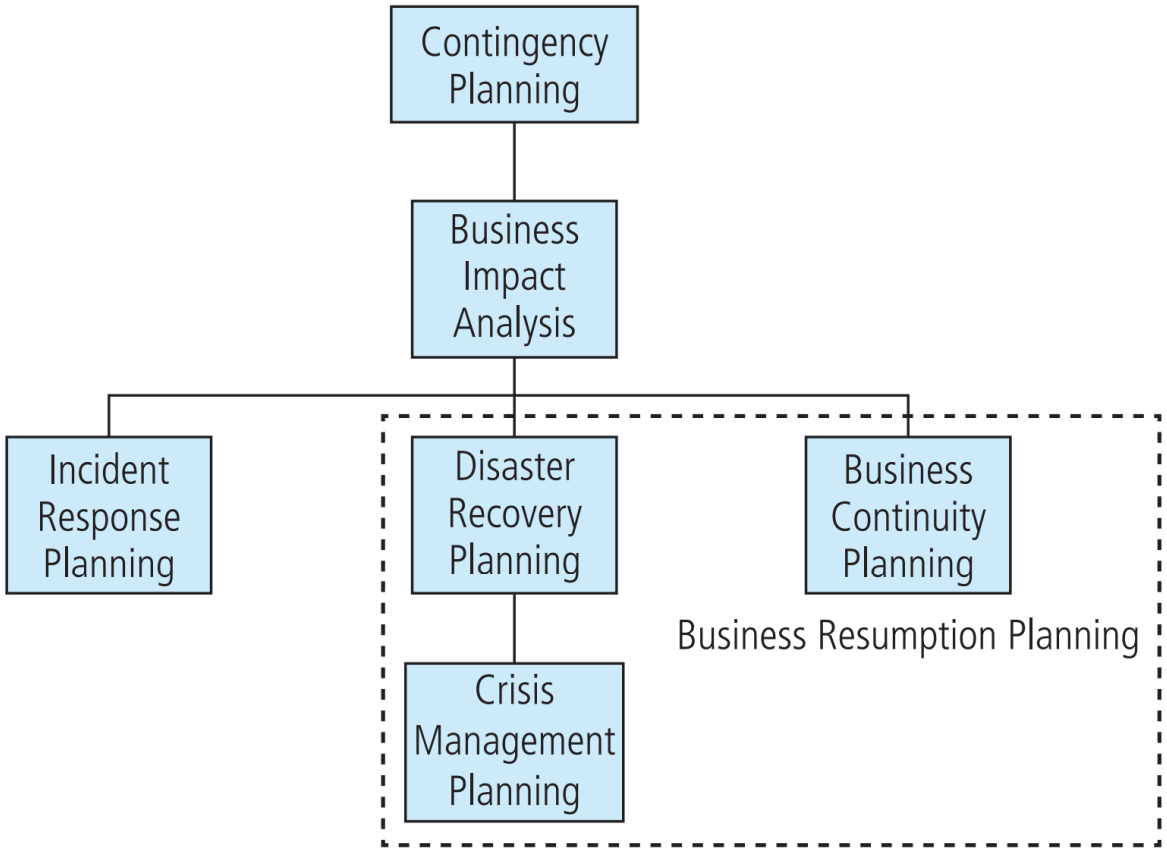
# Components of Contingency Planning …

## ❑ Business continuity planning team (BCPT)

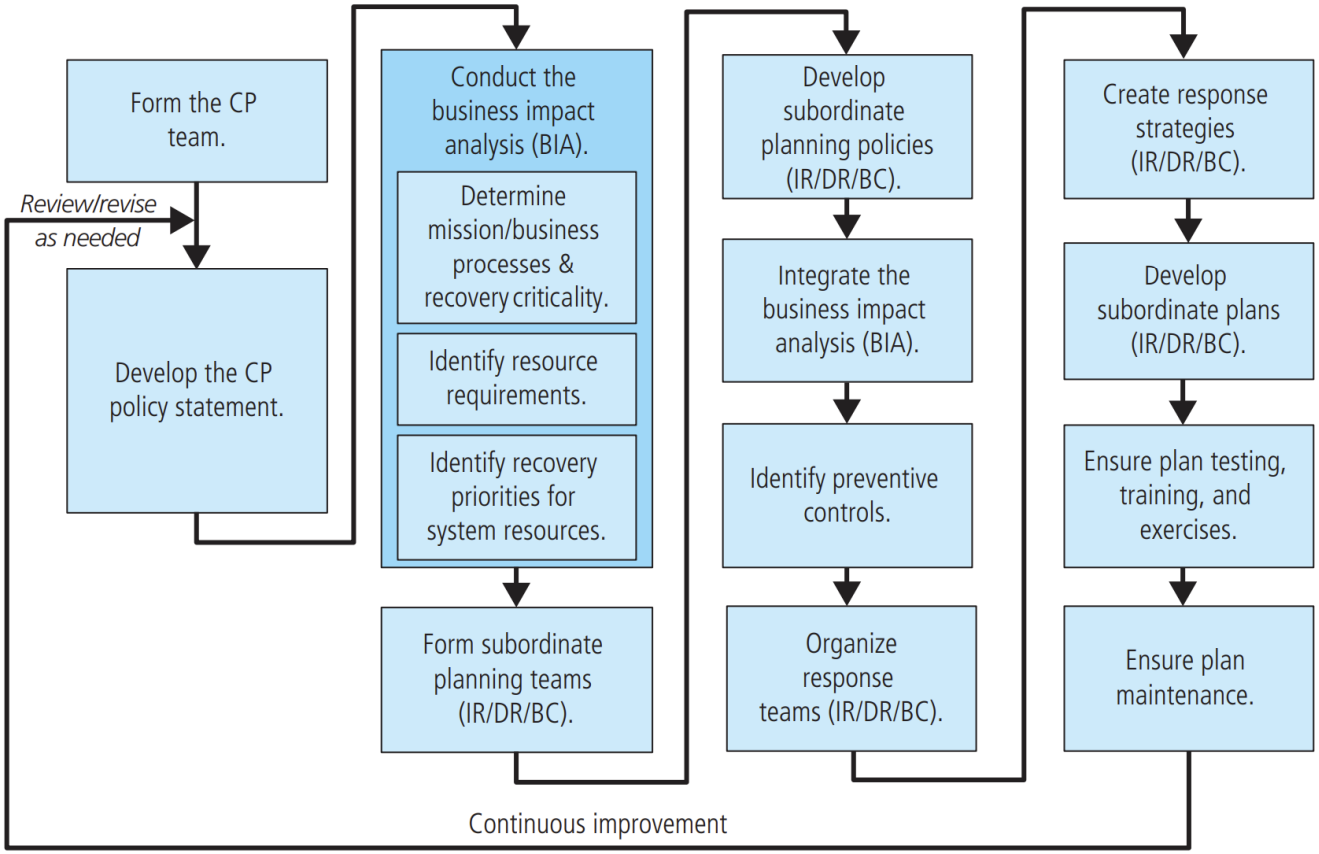
- The team responsible for designing and managing the BC plan of relocating the organization and establishing primary operations at an alternate site until the disaster recovery planning team can recover the primary site or establish a new location.

# Components of Contingency Planning …

- **Crisis management planning team (CMPT)**
  - The individuals from various functional areas of the organization assigned to develop and implement the CM plan.




Contingency planning hierarchies




Contingency planning life cycle

# Summary

- **Cybersecurity contingency planning** focuses on preparing for and responding to cybersecurity incidents and breaches when they occur despite risk management efforts.
  - It involves developing plans and procedures for how the organization will respond to various types of cybersecurity incidents, such as data breaches, malware infections, or denial-of-service attacks.

# Summary …

- Contingency planning includes steps such as incident detection and reporting, containment and eradication of threats, recovery of systems and data, and post-incident analysis to prevent similar incidents in the future.

- The goal of cybersecurity contingency planning is to minimize the impact of cybersecurity incidents on the organization's operations, reputation, and bottom line.

# Summary …

- **Cybersecurity risk management** is about proactively identifying and mitigating cybersecurity risks, while **cybersecurity contingency planning** is about preparing for and responding to cybersecurity incidents when they occur despite risk management efforts.