Information Systems Security [INSY3073]

PART II: Chapters **5** to **8**

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

[INSY 3073]

Chapter 5: Legal, Ethical, and Professional Issues in Information Security

Prepared by:

Lemma Lessa (PhD)

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

FEBRUARY 2025

ICTs  Everything

- ICTs are transforming everything !
  (*rapid, transformational change made possible*)

- We are highly dependent on ICTs to the point where it would be impossible for us to live without it.

Introduction ...

- ICTs are driven by both positive benefits and malicious purposes they can be leveraged for.

- The source of the problem (use for malicious purposes) is not just the technologies themselves rather human behavior is a large part of the problem.

Law and Ethics in Information Security

Law Vs. Ethics

- *Law consists of a set of rules and regulations*
- *Ethics comprises of guidelines and principles that inform people about how to live or how to behave in a particular situation.*

Law and Ethics …

- **Laws** - the rules that members of a society create to balance the individual rights to self-determination against the needs of the society as a whole.

- **Ethics** are based on cultural mores (customs/values). Some ethical standards are universal. For example, murder and theft are generally prohibited in ethical and legal standards throughout the world.

- The key difference between laws and ethics is that laws carry the authority of a governing body and ethics do not.

Law and Ethics …

- As a future information security professional or IT professional with security responsibilities, you must understand the scope of an organization's legal and ethical responsibilities.

- The information security professional plays an important role in an organization's approach to managing responsibility and liability for privacy and security risks.
  - In modern societies, laws are enforced in civil courts, where large damages can be awarded to accusers who bring suits against organizations.

What if an organization does not support or encourage strong ethical conduct on the part of its employees?

Organizational Liability …

- If an employee, acting with or without authorization, performs an illegal or unethical act, causing some degree of harm, the organization can be held financially liable for that action.

Organizational Liability

- An organization increases its liability if it refuses to take measures - due care - to make sure that every employee knows what is acceptable and what is not, and the consequences of illegal or unethical actions.
- Due diligence requires that an organization make a valid and ongoing effort to protect others.

Organizational Liability ...

- It is vital that you understand the legal environment, scope of an organization's legal and ethical responsibilities.
- Educating employees and management about their legal and ethical obligations and the proper use of information technology and information security.
  - To minimize the organization's liabilities

Organizational Liability …

- Even if there is no breach of criminal law in a case, there can still be liability - legal and financial responsibility. Liability includes the legal obligation to make restitution - to pay penalties or fines for wrongs committed.

- If an employee performs an illegal or unethical act that causes some degree of harm, the employer may be held financially liable for that action, regardless of whether the employer authorized the act.

Organizational Liability ...

- An organization increases its liability if it refuses to take measures known as due care (or a standard of due care). Similarly, due diligence requires that an organization make a valid attempt to continually maintain this level of effort.

- **Due care** means the organization acts legally and ethically.

- **Due diligence** means organization ensures compliance with this level of expected behavior, essentially the management of due care.

Organizational Liability ...

- **Due care** involves implementing and maintaining appropriate policies, procedures, standards, and controls that align with the organization's risk appetite and regulatory requirements.

- **Due diligence** refers to the ongoing process of monitoring and reviewing the effectiveness of the due care measures.

Organizational Liability …

- Given the Internet's global reach, those who could be injured or wronged by an organization's employees might live anywhere in the world.

- A court can assert its authority over an individual or organization if it can establish jurisdiction. This is sometimes referred to as long-arm jurisdiction when laws are stretched to apply to parties in distant locations. Trying a case in the injured party's home area is usually favorable to the injured party.

  - **Jurisdiction** - The **power to make legal decisions and judgments**; also, the domain or area within which an entity such as a court or law enforcement agency is empowered to make legal decisions and perform legal actions.

In general, it is difficult to enforce Information security (Cyber security) laws. Why?

The legal environment can influence the organization to a greater or lesser extent, depending on the nature of the organization and the scale on which it operates.

Types of Law

- **Civil law** (also known as private law) pertains to relationships between and among individuals and organizations.
- **Criminal law** addresses violations harmful to society and is actively enforced and prosecuted by **the state**.

Privacy Issues

- Many organizations collect, trade, and sell personal information as a commodity, and many individuals are becoming aware of these practices and looking to the governments to protect their privacy.
- Today, the aggregation of data from multiple sources permits unethical organizations to build databases with alarming quantities of personal information.

Policy Versus Law

- Within an organization, information security professionals help maintain security via the establishment and enforcement of policy.
- Policies function as laws within the operational boundaries of an organization.
  - These policies come with penalties, judicial practices, and sanctions to require compliance.

Policy Versus Law …

- Because policies function as laws, they must be crafted and implemented with the same care to ensure that they are complete, appropriate, and fairly applied to everyone in the workplace.

- The difference between a policy and a law, however, is that ignorance of a policy is an acceptable defense, whereas ignorance of the law is not.

Policy Versus Law …

- Policies must be able to stand up in court if challenged, because if an employee is punished or fired based on a policy violation, they may challenge the action, and most likely in court.

- Thus, for a policy to be enforceable, it **must meet the following five criteria**:

Policy Versus Law …

- **Dissemination (distribution)** - The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.

- **Review (reading)** - The organization must be able to demonstrate that it disseminated the document in an understandable form, including versions for employees who are illiterate, reading impaired, and unable to read English. Common techniques include recordings of the policy in English and alternate languages.

Policy Versus Law …

- **Comprehension (understanding)** - The organization must be able to demonstrate that the employee understands the requirements and content of the policy. Common techniques include quizzes and other assessments.

- **Uniform enforcement** - The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Policy Versus Law …

- **Compliance (agreement)** - The organization must be able to demonstrate that the employee agreed to comply with the policy through act or affirmation. Common techniques include login banners, which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.

- **Only when all of these conditions are met can an organization penalize employees who violate a policy without fear of successful legal retribution.**

Types of Law …

- Regardless of how you categorize laws, it is important to understand which laws and regulations are relevant to your organization and what the organization needs to do to comply.

Computer Crime

- **Cybercrime** encompasses a wide range of criminal activities that are carried out using digital devices and/or networks.
  - These crimes involve the use of technology to commit fraud, identity theft, data breaches, computer viruses, scams, and expanded upon in other malicious acts.

Computer Crime…

- The severity of the penalty depends on the value of the information obtained and whether the offense is judged to have been committed for the following reasons:
  - For purposes of commercial advantage
  - For private financial gain
  - In furtherance of a criminal act

Computer Crime Law …

- Related to privacy identity theft can occur when someone steals a victim's personally identifiable information (PII) and uses it to purchase goods and services or conduct other actions while posing as the victim.

International Laws and Legal Bodies

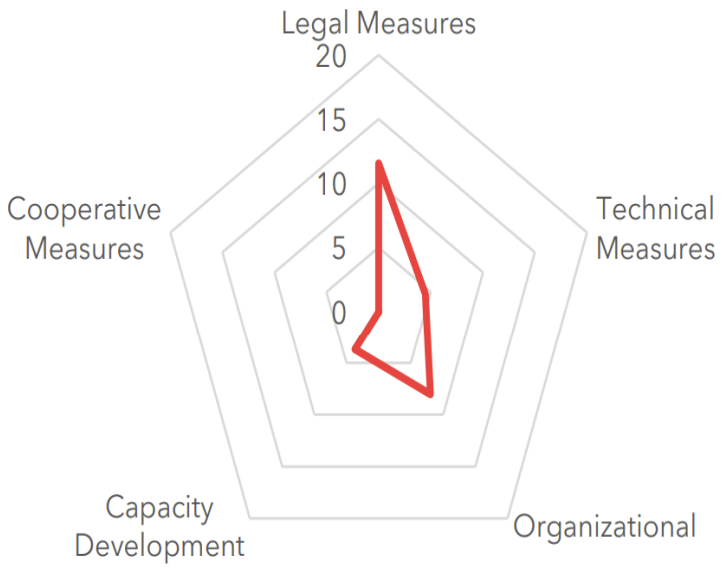
European Council Cyber-Crime Convention

- The Council of Europe's Convention on Cybercrime - November 23, 2001.
  - The Convention is the first international treaty designed to address several categories of crimes committed via the Internet and other computer networks.
  - The overall goal of the convention is to simplify the acquisition of information for law enforcement agents in relation to international crimes, as well as the extradition/deportation process.

Digital Millennium Copyright Act (DMCA)

- US-based international effort to reduce the impact of copyright, trademark, and privacy infringement, especially via the removal of technological copyright protection measures.

Ethiopia (Federal Democratic Republic of)



Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures

Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
27.74	11.56	4.46	8.03	3.69	0.00

Source: ITU Global Cybersecurity Index v4, 2020

National laws that provide for privacy and data protection rules

- **The Constitution**
- Freedom of the Mass Media and Access to Information Proclamation No. 590/2008 ('the Mass Media Proclamation')
- Civil Code of the Empire of Ethiopia Proclamation No. 165/1960 ('the Civil Code')
- Criminal Code of the Federal Democratic Republic of Ethiopia Proclamation No.414/2004 ('the Criminal Code')
- Criminal Procedure Code of the Empire of Ethiopia, 1961 ('the Criminal Procedure Code')

National laws that provide for privacy and data protection rules …

- The Food, Medicine, and Healthcare Administration and Control Council of Ministers Regulation ('the Regulation')
- The Communications Service Proclamation No.1148/2019 ('the Communications Service Proclamation')
- Computer Crime Proclamation No. 958/2016 ('the Computer Crime Proclamation')
- Registration of Vital Events and National Identification Cards Proclamation No. 760/2012 ('the Registration of Vital Events and National Identity Card Proclamation')
- Federal Tax Administration Proclamation No.983/2016 ('the Federal Tax Administration Proclamation')

National laws that provide for privacy and data protection rules …

- Authentication and Registration of Documents' Proclamation No.922/2015 ('the Documents Authentication and Registration Proclamation')
- Electronic Signature Proclamation No.1072/2018 ('the Electronic Signature Proclamation')
- Electronic Transaction Proclamation No.1205/2020 ('the Electronic Transaction Proclamation')
- Licensing and Authorization of Payment Instrument Issuers Directive No. ONPS/01/2020 ('the Licensing and Authorization of Payment Instrument Issuers Directive'); and
- Financial Consumer Protection Directive No. FCP/01/2020 ('the Financial Consumer Protection Directive').

Ethics and Information Security

- Many professionally regulated disciplines have explicit rules that govern the ethical behavior of their members.
  - For example, doctors and lawyers who commit egregious violations of their professions' canons of conduct can have their legal ability to practice revoked.

Ethics and Information Security

- Unlike the medical and legal fields, however, the information technology and information security fields do not have binding codes of ethics.
- Instead, professional associations such as the ACM and ISSA, and certification agencies such as (ISC) and ISACA, work to maintain ethical codes of conduct for their respective memberships.
- While these professional organizations can prescribe ethical conduct, they do not have the authority to banish violators.

The Ten Commandments of Computer Ethics from the Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Ethical Differences Across Cultures

- Cultural differences can make it difficult to determine what is ethical and what is not - especially when it comes to the use of computers.

- Studies on ethics and computer use reveal that people of different nationalities have different perspectives; difficulties arise when one nationality's ethical behavior violates the ethics of another national group.

Ethics and Education

- Attitudes toward the ethics of computer use are affected by many factors other than nationality.
- Differences are found among people within the same country, within the same social class, and within the same company.
- Education is the overriding factor in leveling ethical perceptions within a small population.
- Proper ethical and legal training is vital to creating an informed and well-prepared system user.

Causes of unethical and illegal behavior

- **Ignorance** - Ignorance of the law is no excuse; however, ignorance of policy and procedures is.
- The first method of deterrence is education, which is accomplished by designing, publishing, and disseminating an organization's policies and relevant laws, and by obtaining agreement to comply with these policies and laws from all members of the organization.
  - Reminders, training, and awareness programs keep policy information in front of employees to support retention and compliance.

Causes of unethical and illegal behavior

- **Accident** - People who have authorization and privileges to manage information within the organization are most likely to cause harm or damage by accident.
- Careful planning and control help prevent accidental modification to systems and data.

Causes of unethical and illegal behavior

- **Intent** - Criminal or unethical intent goes to the state of mind of the person performing the act; it is often necessary to establish criminal intent to successfully prosecute offenders.
- Protecting a system against those with intent to cause harm or damage is best accomplished by means of technical controls, and vigorous litigation or prosecution if these controls fail.

Causes of unethical and illegal behavior

- Whatever the cause of illegal, immoral, or unethical behavior, one thing is certain: Information security personnel must do everything in their power to deter these acts and to use policy, education and training, and technology to protect information and systems.
- Many security professionals understand the technology aspect of protection but underestimate the value of policy.

Causes of unethical and illegal behavior

- Laws, policies, and their associated penalties only provide deterrence if three conditions are present:

- **Fear of penalty** - Potential offenders must fear the penalty. Threats of informal warnings or verbal warnings do not have the same impact as the threat of imprisonment or penalty of pay.
- **Probability of being apprehended** - Potential offenders must believe there is a strong possibility of being caught.
- **Probability of penalty being applied** - Potential offenders must believe that the penalty will be administered.

Codes of Ethics of Professional Organizations

- Many professional organizations have established codes of conduct or codes of ethics that members are expected to follow.
- Codes of ethics can have a positive effect on people's judgment regarding computer use.
- Unfortunately, many employers do not encourage their employees to join these professional organizations.

Codes of Ethics of Professional Organizations

- Security professionals have a responsibility to act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society.
- Likewise, it is the organization's responsibility to develop, disseminate, and enforce its policies.

Major IT and InfoSec Professional Organizations

Professional Organization	Web Resource Location	Description and Link to Code of Ethics
ACM	*www.acm.org*	The ACM is the oldest computing society; its code of ethics requires members to perform their duties in a manner befitting an ethical computing professional. *www.acm.org/code-of-ethics*
ISACA	*www.isaca.org*	Promotes a code of ethics for its certification holders, including CISA and CISM. *www.isaca.org/credentialing/code-of-professional-ethics*
ISSA	*www.issa.org*	Professional association of security professionals. *www.members.issa.org/page/CodeofEthics*
$(ISC)^2$	*www.isc2.org*	Promotes a code of ethics based on four canons for its certification holders, including CISSP and SSCP. *www.isc2.org/Ethics*
SANS GIAC	*www.giac.org*	Promotes a code of ethics based on respect for the public, the certification, and its certification holders, including GIAC and GSE. *www.giac.org/about/ethics*
EC-Council	*www.eccouncil.org*	Promotes a code of ethics for its certification holders, including CCISO and CEH. *www.eccouncil.org/code-of-ethics/*

Information Systems Security

[INSY 3073]

Chapter 6: Security and Personnel

Prepared by:

Lemma Lessa (PhD)

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

FEBRUARY 2025

Security and Personnel

Humans are the weakest link in the information security chain and are the root cause of numerous security incidents in organizations.

What do you understand by this statement?

Security and Personnel

- Maintaining a secure environment requires that:
  - ✓ The InfoSec department be carefully structured and staffed with appropriately credentialed personnel.
  - ✓ The proper procedures be integrated into all human resources activities, including hiring, training, promotion, and termination practices.

Security and Personnel …

- The general management community of interest should learn more about the requirements and qualifications for both information security positions and relevant IT positions.
- Upper management should learn more about information security budgetary and personnel needs.
- The IT and general management communities of interest must grant the information security function (and CISO) an appropriate level of influence and prestige.

What are key skills and requirements for information security positions

Qualifications and Requirements

- Individuals who have the following abilities:
  - Understand how organizations are structured and operated
  - Recognize that InfoSec is a management task that cannot be handled with technology alone
  - Work well with people in general, including users, and communicate effectively using both strong written and verbal communication skills
  - Acknowledge the role of policy in guiding security efforts

Qualifications and Requirements …

- Individuals who have the following abilities (Cont'd):
  - Understand the essential role of information security education and training, which helps make users part of the solution, rather than part of the problem
  - Perceive the threats facing an organization, understand how these threats can become transformed into attacks, and safeguard the organization from information security attacks

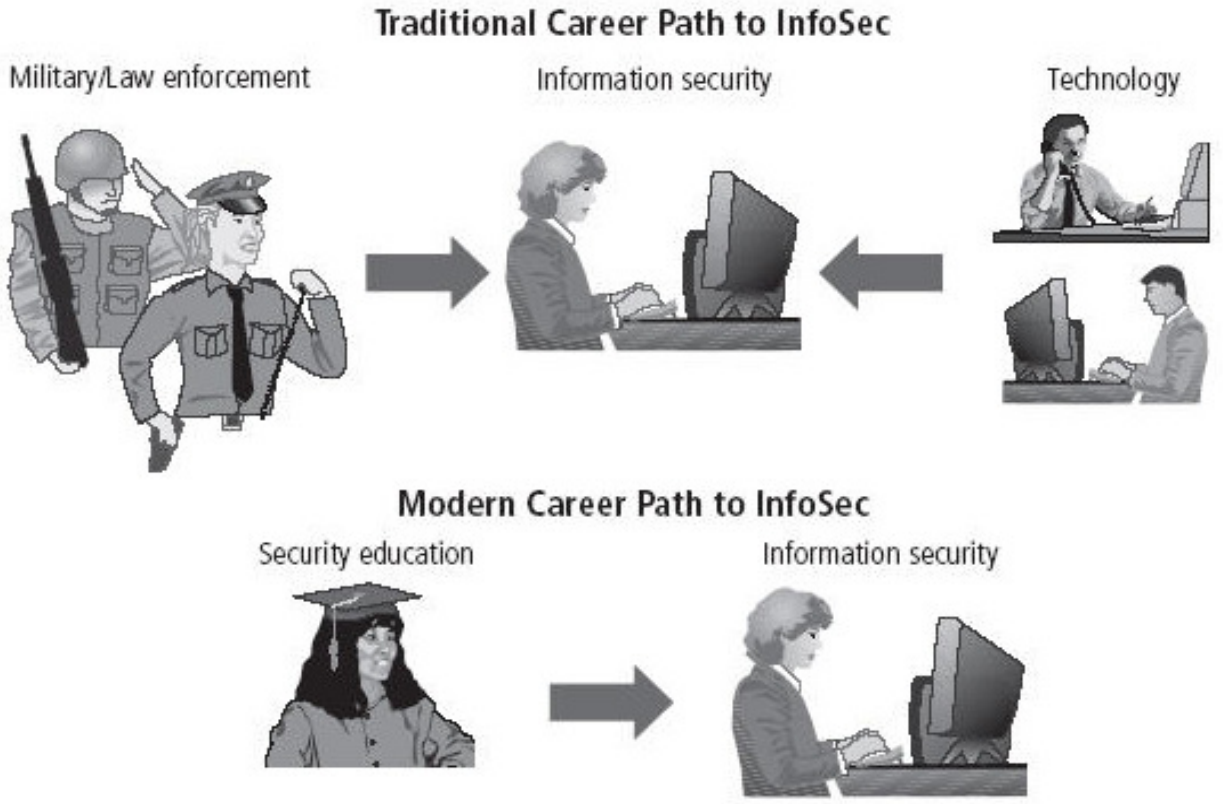
Qualifications and Requirements …

- Individuals who have the following abilities (Cont'd):
  - Understand how technical controls can be applied to solve specific information security problems.
  - Demonstrate familiarity with the mainstream information technologies
  - Understand IT and InfoSec terminology and concepts

Entering the Information Security Profession

- Many information security professionals enter the field after having prior careers in law enforcement or the military, or careers in other IT areas, such as networking, programming, database administration, or systems administration
- Organizations can foster greater professionalism in the information security discipline by clearly defining their expectations and establishing explicit position descriptions.

Information Security Career Paths



Information Security Positions

- Information security positions can be classified into one of three areas: those that **define**, those that **build**, and those that **administer**.

- **Definers provide the policies, guidelines, and standards**
  - The people who do the consulting and the risk assessment, and develop the product and technical architectures
  - Senior people with a broad knowledge, but not a lot of depth
- **Builders are the real techies, who create and install security solutions**
- **Administer are the people who operate and administer the security tools**, the security monitoring function, and the people who continuously improve the processes
  - This is where all the day-to-day, hard work is done

Chief Information Security Officer (CISO)

- The CISO is typically considered the top information security officer in the organization, although the CISO is usually not an executive-level position and frequently reports to the CIO
- Although these individuals are business managers first and technologists second, they must be conversant in all areas of information security, including technology, planning, and policy.

CISO: Qualifications and Position Requirements

- The most common qualification for the CISO is the Certified Information Systems Security Professional (CISSP).
- A graduate degree in criminal justice, business, technology, or another related field is usually required as well.
- A candidate for this position should have experience in security management, as well as in planning, policy, and budgets.

Security Technician

- Security technicians are technically qualified individuals who configure firewalls and IDSs, implement security software, diagnose and troubleshoot problems, and coordinate with systems and network administrators to ensure that security technology is properly implemented.
- The role of security technician is the typical information security entry-level position, albeit a technical one.

Employment Policies and Practices

- The general management community of interest should integrate solid information security concepts across all of the organization's employment policies and practices.
- Including information security responsibilities into every employee's job description and subsequent performance reviews can make an entire organization take information security more seriously.

Hiring

- From an information security perspective, the hiring of employees is laden with potential security pitfalls.
- The CISO, in cooperation with the CIO and relevant information security managers, should establish a dialogue with human resources personnel so that information security considerations become part of the hiring process.

Hiring Issues

Job Descriptions

- Organizations that provide complete job descriptions when advertising open positions should omit the elements of the job description that describe access privileges

Interviews

- In general, information security should advise human resources to limit the information provided to the candidates on the access rights of the position
- When an interview includes a site visit, the tour should avoid secure and restricted sites, because the visitor could observe enough information about the operations or information security functions to represent a potential threat to the organization

Hiring Issues …

- **New Hire Orientation**
  - New employees should receive, as part of their orientation, an extensive information security briefing
- **On-the-Job Security Training**
  - Organizations should conduct periodic security awareness and training activities to keep security at the forefront of employees' minds and minimize employee mistakes
- **Security Checks**
  - A background check should be conducted before the organization extends an offer to any candidate, regardless of job level

Common Background Checks

- Identity checks: personal identity validation
- Education and credential checks: institutions attended, degrees and certifications earned, and certification status
- Previous employment verification: where candidates worked, why they left, what they did, and for how long
- Reference checks: validity of references and integrity of reference sources

Common Background Checks …

- Worker's compensation history: claims from worker's compensation
- Motor vehicle records: driving records, suspensions, and other items noted in the applicant's public record
- Drug history: drug screening and drug usage, past and present
- Medical history: current and previous medical conditions, usually associated with physical capability to perform the work in the specified position.

Common Background Checks …

- Credit history: credit problems, financial problems, and bankruptcy
- Civil court history: involvement as the plaintiff/accuser or defendant/suspect in civil suits
- Criminal court history: criminal background, arrests, convictions, and time served

Contracts and Employment

- Once a candidate has accepted a job offer, the employment contract becomes an important security instrument
- It is important to have these contracts and agreements in place at the time of the hire

Security as Part of Performance Evaluation

- To heighten information security awareness and change workplace behavior, organizations should incorporate information security components into employee performance evaluations.
- Employees pay close attention to job performance evaluations, and including information security tasks in them will motivate employees to take more care when performing these tasks.

Termination Issues

- When an employee leaves an organization, the following tasks must be performed:
  - The former employee's access to the organization's systems must be disabled
  - The former employee must return all removable media
  - The former employee's hard drives must be secured
  - File cabinet locks must be changed
  - Office door locks must be changed
  - The former employee's keycard access must be revoked
  - The former employee's personal effects must be removed from the premises
  - The former employee should be escorted from the premises, once keys, keycards, and other business property have been turned over

Termination Issues …

- In addition to performing these tasks, many organizations conduct an exit interview to remind the employee of any contractual obligations, such as nondisclosure agreements, and to obtain feedback on the employee's tenure in the organization
- Two methods for handling employee outprocessing, depending on the employee's reasons for leaving, are hostile and friendly departures.

What is the implication of hostile and friendly departures on Information security tasks in an organization?

Hostile Departure

- Security cuts off all logical and keycard access, before the employee is terminated.
- The employee reports for work and is escorted into the supervisor's office to receive the bad news.
- The individual is then escorted from the workplace and informed that his or her personal property will be forwarded, or is escorted to his or her office, cubicle, or personal area to collect personal effects under supervision
- Once personal property has been gathered, the employee is asked to surrender all keys, keycards, and other organizational identification and access devices, PDAs, pagers, cell phones, and all remaining company property, and is then escorted from the building

Friendly Departure

- The employee may have tendered notice well in advance of the actual departure date, which can make it much more difficult for security to maintain positive control over the employee's access and information usage
- Employee accounts are usually allowed to continue, with a new expiration date
- The employee can come and go at will and usually collects any belongings and leaves without escort
- The employee is asked to drop off all organizational property before departing.

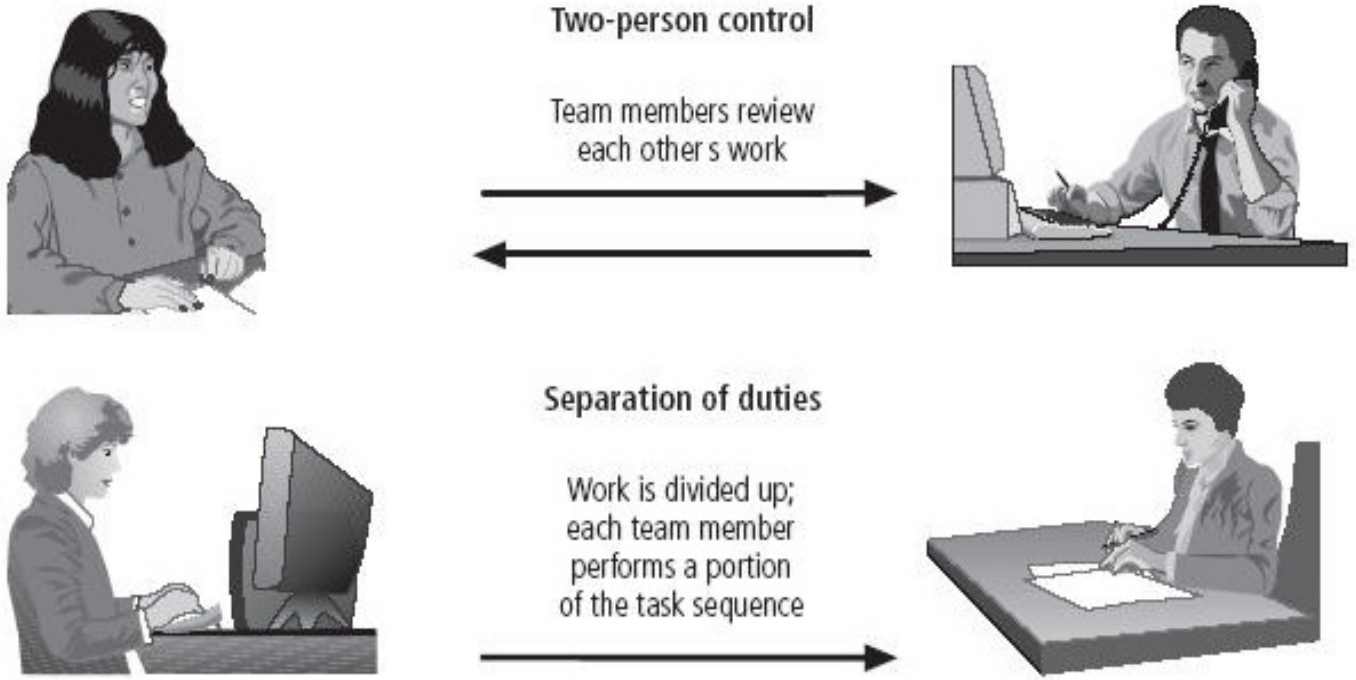
Termination Issues

- In either circumstance, the offices and information used by departing employees must be inventoried, their files stored or destroyed, and all property returned to organizational stores.
  - It is possible that departing employees have collected and taken home information or assets that could be valuable in their future jobs.
  - Only by scrutinizing system logs during the transition period and after the employee has departed, and sorting out authorized actions from system misuse or information theft, can the organization determine whether a breach of policy or a loss of information has occurred.

Personnel Security Control Strategies

- There are various ways of monitoring and controlling employees to minimize their opportunities to misuse information
  - **Separation of duties** is used to make it difficult for an individual to violate information security and breach the confidentiality, integrity, or availability of information
  - **Two-man control** requires that two individuals review and approve each other's work before the task is considered complete.

Personnel Security Control Strategies



Personnel Security Control Strategies

- **Job rotation** is another control used to prevent personnel from misusing information assets
  - Job rotation requires that every employee be able to perform the work of at least one other employee
  - If that approach is not feasible, an alternative is task rotation, in which all critical tasks can be performed by multiple individuals

Personnel Security Control Strategies …

- Both job rotation and task rotation ensure that no one employee is performing actions that cannot be knowledgeably reviewed by another employee.
- For similar reasons, each employee should be required to take a mandatory vacation, of at least one week per year.
- This policy gives the organization a chance to perform a detailed review of everyone's work.

Personnel Security Control Strategies …

- Finally, another important way to minimize opportunities for employee misuse information is to limit access to information **(Least privilege)**.
  - That is, employees should be able to access only the information they need, and only for the period required to perform their tasks
  - This idea is referred to as the principle of least privilege

Personnel Security Control Strategies …

- Least privilege ensures that no unnecessary access to data occurs
- If all employees can access all the organization's data all the time, it is almost certain that abuses—possibly leading to losses in confidentiality, integrity, and availability—will occur

Security of Personnel and Personal Data

- Organizations are required by law to protect sensitive or personal employee information, including personally identifying facts such as employee addresses, phone numbers, Social Security numbers, medical conditions, and even names and addresses of family members
- This responsibility also extends to customers, patients, and anyone with whom the organization has business relationships.

Security Considerations for Non-employees

- Many individuals who are not employees often have access to sensitive organizational information.
- Relationships with individuals in this category should be carefully managed to prevent threats to information assets from materializing.

Temporary Workers

- Because temporary workers are not employed by the organization for which they are working, they may not be subject to the contractual obligations or general policies that govern other employees
- From a security standpoint, access to information for temporary workers should be limited to what is necessary to perform their duties.

Contract Employees

- While professional contractors may require access to virtually all areas of the organization to do their jobs, service contractors usually need access only to specific facilities, and they should not be allowed to wander freely in and out of buildings
- In a secure facility, all service contractors are escorted from room to room, and into and out of the facility.

Contract Employees …

- Any service agreements or contracts should contain the following regulations:
  - The facility requires 24 to 48 hours' notice of a maintenance visit
  - The facility requires all on-site personnel to undergo background checks
  - The facility requires advance notice for cancellation or rescheduling of a maintenance visit

Consultants

- Consultants have their own security requirements and contractual obligations.
- They should be handled like contract employees, with special requirements, such as information or facility access requirements, being integrated into the contract before they are given free access to the facility.
- Just because you pay security consultants, it doesn't mean that protecting your information is their number one priority.
- Always remember to apply the principle of least privilege when working with consultants.

Business Partners

- Businesses sometimes engage in strategic alliances with other organizations to exchange information, integrate systems, or enjoy some other mutual advantage.
- A prior business agreement must specify the levels of exposure that both organizations are willing to tolerate.
- In particular, security and technology consultants must be prescreened, escorted, and subjected to nondisclosure agreements to protect the organization from intentional or accidental breaches of confidentiality.

Business Partners …

- If the strategic partnership evolves into an integration of the systems of both companies, competing groups may be provided with information that neither parent organization expected
  - Nondisclosure agreements are an important part of any such collaborative effort
- The level of security of both systems must be examined before any physical integration takes place, as system connection means that vulnerability on one system becomes vulnerability for all linked systems.

Information Systems Security

[INSY 3073]

Chapter 7: Security Tools and Technologies

Prepared by:

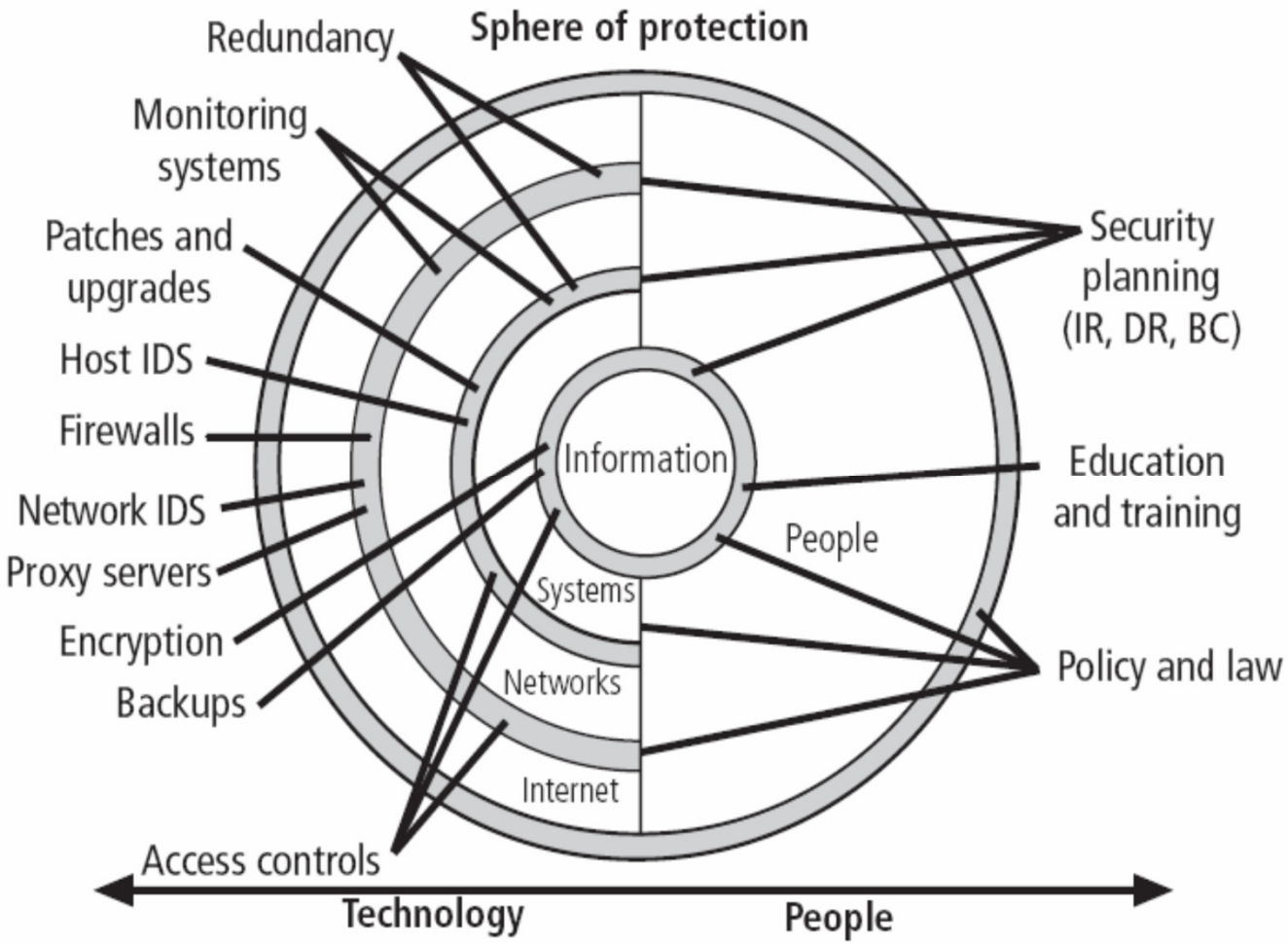
Lemma Lessa (PhD)

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

FEBRUARY 2025

Introduction

- Technical controls are an important part of an information security program
- They must be combined with sound policy, education, training, and awareness efforts.


Redundancy
Sphere of protection
Monitoring systems
Patches and upgrades
Host IDS
Firewalls
Network IDS
Proxy servers
Encryption
Backups
Access controls
Information
Systems
Networks
Internet
Security planning (IR, DR, BC)
Education and training
People
Policy and law
Technology
People

Access Control, Firewall and VPN

- Some of the most powerful and widely used technical security mechanisms include:
  - Access controls
  - Firewalls
  - Intrusion detection systems
  - Scanning and analysis tools
  - Encryption systems

Access Control, Firewall and VPN

Access Control, Firewall and VPN

- **Access control** is a process by which systems determine if and how to admit a user into a trusted area of the organization.
- **Mandatory access controls (MACs)** offer users and data owners little or no control over access to information resources.
  - MACs are often associated with a data classification scheme in which each collection of information is rated with a sensitivity level.
  - This type of control is sometimes called lattice-based access control.

Access Control, Firewall and VPN

- **Nondiscretionary access controls** are strictly enforced versions of MACs that are managed by a central authority, whereas **discretionary access controls** are implemented at the discretion or option of the data user.
- All access control approaches rely on identification, authentication, authorization, and accountability.

Access Control, Firewall and VPN

- Authentication is the process of validating an unauthenticated entity's purported identity.
  - The three widely used types of authentication factors are:
    - Something a person knows
    - Something a person has, and
    - Something a person is or can produce.

Access Control, Firewall and VPN

- **Strong authentication** requires a minimum of two authentication mechanisms drawn from two different authentication factors.
- **Biometrics** is the use of a person's physiological characteristics to provide authentication for system access.

Access Control, Firewall and VPN

- Access control encompasses two processes:
  - Confirming the identity of the entity accessing a logical or physical area (authentication)
  - Determining which actions that entity can perform in that physical or logical area (authorization)
- A successful access control approach—whether intended to control physical access or logical access—always consists of both authentication and authorization._

Authentication Mechanisms

- Mechanism types
  - Something you know
  - Something you have
  - Something you are
  - Something you produce
- Strong authentication uses at least two different authentication mechanism types.

Something You Know

- This type of authentication mechanism verifies the user's identity by means of a password, passphrase, or other unique code.
- A password is a private word or combination of characters that only the user should know
- A passphrase is a plain-language phrase, typically longer than a password, from which a virtual password is derived
- A good rule of thumb is to require that passwords be at least eight characters long and contain at least one number and one special character

Something You Have

- This authentication mechanism makes use of something (a card, key, or token) that the user or the system possesses.
  - One example is a dumb card (such as an ATM card) with magnetic stripes
  - Another example is the smart card containing a processor
  - Another device often used is the cryptographic token, a processor in a card that has a display
  - Tokens may be either synchronous or asynchronous

Something You Are

- This authentication mechanism takes advantage of something inherent in the user that is evaluated using biometrics.
  - Most of the technologies that scan human characteristics convert these images to obtain some form of minutiae - unique points of reference that are digitized and stored in an encrypted format.

Something You Do

- This type of authentication makes use of something the user performs or produces.
  - For example, it includes technology related to signature recognition and voice recognition.

Access Control, Firewall and VPN

- **A firewall** is any device that prevents a specific type of information from moving between the outside network, known as the **untrusted network**, and the inside network, known as the **trusted network**.
  - Firewalls operate by evaluating data packet contents against logical rules. This logical set is most commonly referred to as firewall rules, a rule base, or firewall logic.

Access Control, Firewall and VPN

- Dial-up protection mechanisms help secure organizations that use modems for remote connectivity.
  - Kerberos and SESAME are authentication systems that add security to this technology.
- Virtual private networks enable remote offices and users to connect to private networks **securely** over public networks.

Intrusion Detection and Prevention Systems

Intrusion Detection and Prevention Systems

- **Intrusion detection systems (IDSs)** identify potential intrusions and sound an alarm.
  - The more recently developed intrusion detection and prevention systems (IDPSs) also detect intrusions and can take action to defend the network.
  - An IDPS works like a robber alarm by detecting network traffic that violates the system's configured rules and activating an alarm.

Intrusion Detection and Prevention Systems

- A network-based IDPS (NIDPS) monitors network traffic and then notifies the appropriate administrator when a predefined event occurs.
- A host-based IDPS (HIDPS) resides on a particular computer or server and monitors activity on that system.

Intrusion Detection and Prevention Systems

- **Signature-based IDPSs**, also known as knowledge-based IDPSs, examine data traffic for patterns that match signatures - preconfigured, predetermined attack patterns.
- **Anomaly-based IDPSs**, also known as behavior-based IDPSs, collect data from normal traffic and establish a baseline.
  - When an activity is found to be outside the baseline parameters (or clipping level), these IDPSs activate an alarm to notify the administrator.

Intrusion Detection and Prevention Systems

- Selecting IDPS products that best fit an organization's needs is a challenging and complex process.
  - A wide array of products and vendors are available, each with different approaches and capabilities.

Intrusion Detection and Prevention Systems

- Deploying and implementing IDPS technology is a complex undertaking that requires knowledge and experience.
  - After deployment, each organization should measure the effectiveness of its IDPS and then continue with periodic assessments over time.

Intrusion Detection and Prevention Systems

- **Honeypots** are decoy systems designed to lure/trap potential attackers away from critical systems.
  - In the security industry, these systems are also known as decoys, lures, or flytraps.
  - Two variations of this technology are known as honeynets and padded cell systems.

Intrusion Detection and Prevention Systems

- **Trap-and-trace applications** are designed to react to an intrusion event by tracing it back to its source.
  - This process is subject to professional and ethical issues - some people in the security field believe that the back hack in the trace process is as significant a violation as the initial attack.

Intrusion Detection and Prevention Systems

Why IDPS?

- Active intrusion prevention seeks to limit the damage that attackers can perpetrate by making the local network resistant to inappropriate use.

Intrusion Detection and Prevention Systems

- **Scanning and analysis tools** are used to pinpoint vulnerabilities in systems, holes in security components, and unsecured aspects of the network.
  - Although these tools are used by attackers, they can also be used by administrators to learn more about their own systems and to identify and repair system weaknesses before they result in losses.

Introduction To Cryptography

- **Encryption** is the process of converting a message into a form that is unreadable to unauthorized people.

- The science of encryption, known as **cryptology**, encompasses cryptography (making and using encryption codes) and **cryptanalysis** (breaking encryption codes).
  - Cryptology has a long history and continues to change and improve.

- **Cryptography** - The process of making and using codes to secure information._

Information Systems Security

[INSY 3073]

Chapter 8: Implementing Information Security

Prepared by:

Lemma Lessa (PhD)

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

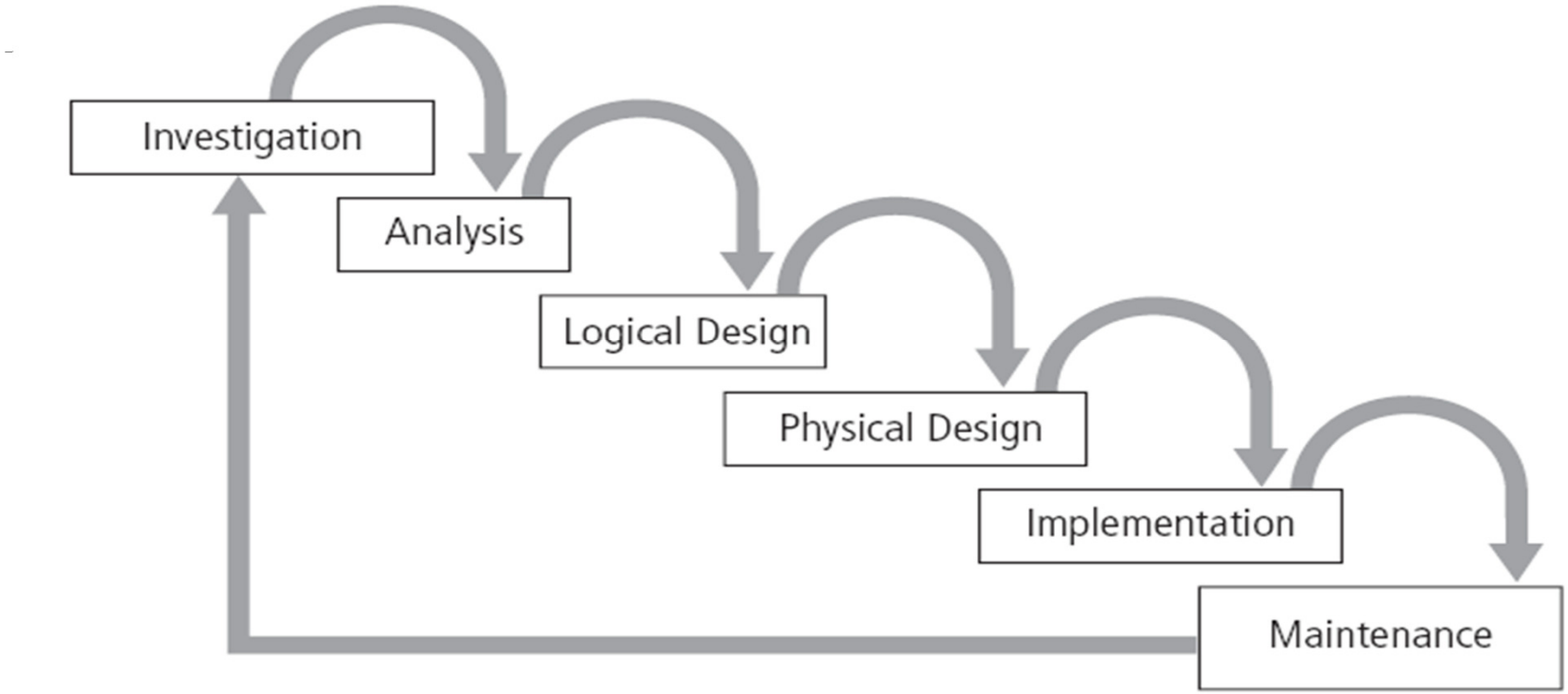
FEBRUARY 2025

Introduction to Information Security Implementation

Information Security Implementation

- Information security should be implemented in every major systems.
- One approach is to ensure that security is a part of the organization's system development methodology.
- Software assurance is a methodological approach to the development of software that seeks to build security into the development life cycle rather than address it at later stages.

Phases of the SecSDLC



Investigation phase in the SecSDLC

- Often begins as a directive from management specifying the process, outcomes, and goals of the project and its budget.
- Teams assembled to analyze problems, define scope, specify goals, and identify constraints
- A feasibility analysis determines whether the organization has the resources and commitment to conduct a successful security analysis and design.
- Frequently begins with the affirmation or creation of security policies

Analysis phase in the SecSDLC

- An analysis of existing security policies or programs is conducted along with known threats and current controls.
  - Includes an analysis of relevant legal issues that could affect the design of the security solution.
- Risk management begins in this stage.

Design phase in the SecSDLC

- This phase consists of two distinct phases:
  - Logical design phase - The information gained from the analysis phase is used to begin creating a systems solution for a business problem.
    - It is the blueprint for the desired solution.
    - It is implementation-independent (ie., it contains no reference to specific technologies, vendors, or products.

Design phase in the SecSDLC

- This phase consists of two distinct phases: …
  - Physical design phase - team members evaluate the technology needed to support the security blueprint, generate alternative solutions, and agree upon a final design.
    - Specific technologies are selected to support the alternatives identified and evaluated in the logical design.

Implementation phase in the SecSDLC …

- This phase involves modifying the configuration and operation of the organization's information systems to make them more secure.
  - Such changes include those to procedures, people, hardware, software, and data.

Implementation phase in the SecSDLC

- The security solutions are acquired, tested, implemented, and tested again.
- Personnel issues are evaluated, and specific training and education programs are conducted.
- The major steps in executing the project plan are planning the project, supervising tasks and action steps within the plan, and wrapping up the plan.

Information Security Implementation

- Each organization determines its own project management methodology for IT and information security projects.
  - Whenever possible, an organization's information security projects should be in line with its project management practices.

Information Security Implementation

- Planning for the implementation phase involves the creation of a detailed project plan.
  - The plan can be prepared with a simple desktop PC spreadsheet program or with more complex project management software.
  - The project plan can be created by using a simple planning tool such as the Work Breakdown Structure (WBS).

Information Security Implementation

- The WBS involves addressing major project tasks and their related attributes, including the following:
  - Work to be accomplished (activities and deliverables)
  - Individual employees or skill sets assigned to perform the task
  - Start and end dates for the task, when known

Information Security Implementation

- The WBS involves addressing major project tasks and their related attributes, including the following: …
  - Amount of effort required for completion, in hours or days
  - Estimated capital expenses for the task
  - Estimated noncapital expenses for the task
  - Identification of task interdependencies

Information Security Implementation

- **Constraints / considerations** should be addressed when developing the project plan.
  - Considerations include those for finances, procurement, priority, time and scheduling, staffing, scope, organizational feasibility, training and indoctrination, change control, and technology governance.

Information Security Implementation

- Organizations usually designate a professional project manager to lead a security information project.
- Alternatively, some organizations designate a champion from a senior level of general management or a senior IT manager, such as the CIO.

Information Security Implementation

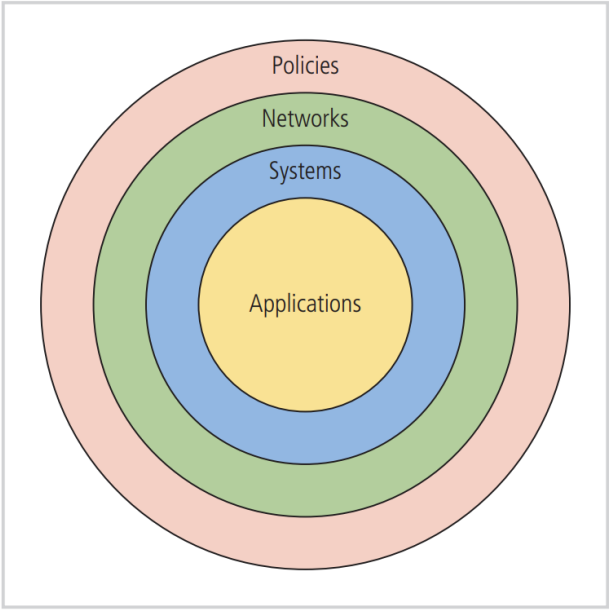
- Once a project is underway, it can be managed to completion using a process known as a negative feedback loop or cybernetic loop.
  - This process involves **measuring variances from the project plan and then taking corrective action when needed**.

Information Security Implementation

- The four common conversion strategies for performing this changeover are as follows:
  - Direct changeover
  - Phased implementation
  - Pilot implementation
  - Parallel operations

Information Security Implementation

- The bull's-eye model is a proven method for prioritizing a program of complex change.
  - Using this method, the project manager can address issues from the general to the specific and focus on systematic solutions instead of individual problems.



Information Security Implementation

- When the expense and time required to develop an effective information security program is beyond the reach of an organization, it should outsource the program to competent professional services.
  - Technology governance is a complex process that an organization uses to manage the impacts and costs of technology implementation, innovation, and obsolescence.

Information Security Implementation

- As with any project, certain aspects of change must be addressed.
  - The change control process is a method that medium-sized and large organizations use to deal with the impact of technical change on their operations.
- In any major project, the prospect of moving from the familiar to the unfamiliar can cause employees to resist change, consciously or unconsciously.

አመሰግናለሁ!


danke
謝謝
tesekkur ederim
thank you
gracias
dziękuję
obrigado
sukriya
merci