CH1:

Policy: A definite course of action or procedure selected from among alternatives and in light of given conditions to guide and determine present and future decisions

Information Security Policy: A document that states how an organization plans to protect its information assets and information systems and ensure compliance with legal and regulatory requirements

Corporate culture classifications: Negative, Neutral, Positive

Asset: Resource with a value

Information asset: Any information item, regardless of storage format, that represents value to the organization (Customer data, employee records, IT information, reputation, and brand)

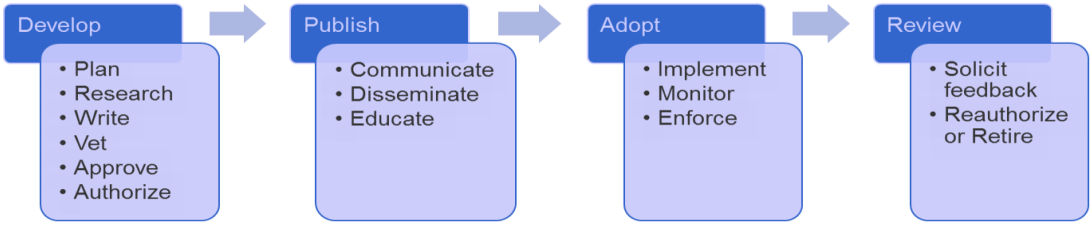
Successful Policy Characteristics:

- Endorsed: Management supports the policy
- Relevant: The policy is applicable and supports the goals of the organization
- Realistic: The policy makes sense
- Attainable: The policy can be successfully implemented
- Adaptable: The policy can be changed
- Enforceable: Controls that can be used to support and enforce the policy exist
- Inclusive: The policy scope includes all relevant parties

two major information security-related legislations were introduced in Saudi Arabia:

- Anti-Cyber Crime ACT.
- Electronic Transactions ACT

Information Security Policy Lifecycle:



CH2

Policy Hierarchy: The relationship between a policy and its supporting documents.

Policies supporting documents:

Standards:	• Dictate specific minimum requirements in policies. • They are specific. • Determined by management. • Can be changed without the Board of Director authorization. • Standards change more often than policies.
Baselines:	• An aggregate of implementation standards and security controls for a specific category or grouping • (for example, Windows 7, smartphones, and so on)
Guideline:	• Suggestions for the best way to accomplish a given task. • Not mandatory. • Created primarily to assist users in their goal to implement the policy.
Procedures:	• Method, or set of instructions, by which a policy is accomplished. • A step---by---step approach.
Plans and Programs:	• Provide strategic and tactical instructions on how to execute an initiative or respond to a situation • Plans and programs are used interchangeably • Plans are closely related to policies

Four commonly used formats for procedures:

- Simple Step: Lists sequential actions. There is no decision making.
- Hierarchical: Includes both generalized instructions for experienced users and detailed instructions for novices.
- Graphic: This format uses either pictures or symbols to illustrate the step.
- Flowchart: Used when a decision-making process associated is with the task.

How standard differs from policy?

Standards serve as specifications for the implementation of policy and dictate mandatory requirements. Example:

- Password Policy: All users must have a unique user ID and password that conforms to the company password standard.
- Password Standard: Minimum of eight upper- and lowercase alphanumeric characters

What are the different types of policy formats?

- Singular policy: Several individual documents?
- Consolidated policy section: One document with multiple sections?

Advantage and Disadvantage of Singular policy and Consolidated policy section

	Singular policy	Consolidated policy section
Advantage	each policy document can be short, clean and crisp, and targeted to its intended audience.	it presents a composite management statement in a single voice.
Disadvantage	need to manage multiple policy documents and the chance that they will become fragmented and lose consistency.	is the potential size of the document and the reader challenge of locating applicable sections.

Policy Document Components:

Component	Purpose
Version control	To track changes
Introduction	to frame the document
Policy heading	To identify the topic
Policy goals and objectives	to convey intent
Policy statement	Mandatory directive
Policy Exceptions	To acknowledge exclusions
Policy enforcement clause	Violation sanctions
Administrative notations	Additional information
Policy definitions	Glossary of terms

Writing Style and Technique:

- Sets the first impression
- Policies should be written using plain language
- Simplest, most straightforward way to express an idea
- Follow the Plan Language Action and Information Network (PLAIN) guidelines

The Plan Language Action and Information Network (PLAIN) guidelines:

• Write for your audience	• Don't use jargon or technical terms
• Write short sentences	• Use active voice
• Limit a paragraph to one subject	• Use must not shall
• Be concise	• Use words and terms consistently through your document

CH3:

What is the objective of information security?

CIA Triad or CIA security model (Confidentiality, Integrity, and Availability).

- Protecting the CIA triad means protecting the assets of the company

The relationship between information security and the CIA triad as follows: information security means protecting information and information systems in order to provide Integrity, Confidentiality and Availability.

What Is Confidentiality?

- Only authorized users should gain access to information
- Information must be protected when it is used, shared, transmitted, and stored
- Information must be protected from unauthorized users both internally and externally

The threats to confidentiality include:

❖ Hackers and hacktivists	❖ Malicious Code (Virus, worms, Trojans)
❖ Shoulder surfing	❖ Unauthorized employee activity
❖ Lack of shredding of paper documents	❖ Improper access control

The information security goal of confidentiality is to protect information from unauthorized access and misuse

What Is Integrity: Protecting data, processes, or systems from intentional or accidental unauthorized modification

- Data integrity: A requirement that information and programs are changed only in a specified and authorized manner
- System integrity: A requirement that a system "performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Threats to data integrity include:

❖ Human error	❖ Improper access control
❖ Hackers	❖ Malicious code
❖ Unauthorized user activity	❖ Interception and alteration of data during transmission

Controls that can be deployed to protect data integrity include:

- Access controls: Encryption, Digital signatures
- Process controls: Code testing
- Monitoring controls: File integrity monitoring, Log analysis
- Behavioral controls: Separation of duties, Rotation of duties, End user security training

What Is Availability: Availability is the assurance that the data and systems are accessible when needed by authorized users.

Threats to data availability include:

❖ Natural disaster	❖ Human errors
❖ Hardware failures	❖ Distributed Denial of Service attacks
❖ Programming errors	❖ Loss of power

Service Level Agreement (SLA): is a type of agreement between a service provider and a customer that specifically addresses availability of services

Five A's of Information Security:

- Accountability: All actions should be traceable to the person who committed them
- Assurance: Security measures need to be designed and tested to ascertain that they are efficient and appropriate
- Authentication: It is the positive identification of the person or system access to secured information and/or system
- Authorization: Act of granting users or systems actual access to information resources
- Accounting: Defined as the logging of access and usage of resources

Who Is Responsible for CIA?

- Information owner: an information owner has the authority and responsibility for ensuring that information is protected, from creation through destruction

Who Is Responsible to safeguard the systems?

- information custodians: system administrators, webmasters, and network engineers

Security framework is a collective term given to guidance on topics related to:

- information systems security
- predominantly regarding the planning
- Implementing
- Managing and auditing of overall information security practices

What are the widely used information security frameworks?

- Information Technology and Security Framework by NIST
- Information Security Management System by ISO

CH4:

Two approaches to information security

- Parallel approach: assigns responsibility for being secure to the IT department, views compliance as discretionary, and has little or no organizational accountability
- Integrated approach: recognizes that security and success are intertwined

Versions of information security policies: User version, Vendor version

Who Authorizes Information Security Policy? executive management.

Change drivers are events that modify how a company does business, Examples: new products, services or technology

Evaluating Information Security Polices:

- Standardized methodologies such as audits and maturity models can be used as evaluation and reporting mechanisms
- Organizations may choose to conduct these evaluations using in-house personnel or engage independent third parties

Audit:

- Systematic, evidence-based evaluation
- Include interviews, observation, tracing documents to management policies, review or practices, review of documents, and tracing data to source documents
- Audit report containing the formal opinion and findings of the audit team is generated at the end of the audit

Capability maturity model (CMM) is used to evaluate and document process maturity for a given area.

Information Security Governance: is the process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors.

Effective security requires the

- Active involvement
- Cooperation
- Collaboration of stakeholders
- Decision makers, and the user community

Chief information security officer (CISO): coordinates and manages security efforts across the company, including IT, human resources (HR), communications, legal, facilities management, and other groups.

Information Security Steering Committee (ISC): provides a forum to communicate, discuss, and debate on security requirements and business integration.

factors influence information security decision making and policy creation:

- ❖ Guiding principles
- ❖ Regulatory requirements
- ❖ Risk associated with achieving business objectives

Risk: The potential of undesirable or unfavorable outcome from a given action

Risk tolerance: How much undesirable outcome the risk taker is willing to accept

Risk appetite: The amount of risk an entity is willing to accept in pursuit of its mission

Risk Assessment: Evaluate what can go wrong and the likelihood of a harmful event occurring

Risk assessment involves

1. Identifying the inherent risk based on relevant threats, threat sources, and related vulnerabilities
   - Inherent risk: The level of risk before security measure are applied
   - Threat: Natural, environmental, or human event that could cause harm
   - Vulnerability: A weakness that could be exploited by a threat
2. Determining the impact of a threat if it occurs
   - Impact: The magnitude of a harm
3. Calculating the likelihood of occurrence
4. Determining residual risk
   - Residual risk: The level of risk after security measures are applied

Components of a risk assessment:

- ❖ Defined process
- ❖ Assessment approach
- ❖ Standardized analysis

Risk Assessment Methodologies:

- ❖ Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
- ❖ Factor Analysis of Information Risk (FAIR)
- ❖ NIST Risk Management Framework (RMF)

Risk Management: is the process of determining an acceptable level of risk (risk appetite and tolerance), calculating the current level of risk (risk assessment), accepting the level of risk (risk acceptance), or taking steps to reduce risk to the acceptable level (risk mitigation).

acceptable level of risk:

- ❖ Risk acceptance: indicates that the organization is willing to accept the level of risk associated with a given activity.
- ❖ Risk mitigation: is a process of reducing, sharing, transferring, or avoiding risk.
  - Risk reduction: Process of control to lower the residual risk
    - Offensive Control: reducing the vulnerabilities by enhanced training or applying security patch
    - Defensive control: respond to threat source such as sensor sending an alert
  - Risk transfer: shifts the entire risk responsibility or liability from one organization to another organization
  - Risk sharing: shifts a portion of risk responsibility or liability to other organizations
  - Risk avoidance: involves taking specific actions to eliminate

CH5:

What is an information asset?

- ❖ A definable piece of information, stored in any manner, and recognized as having value to the organization
- ❖ It includes raw, mined, developed, and purchased data

Information Systems: Provide a way and a place to process, store, transmit, and communicate the information

Who is Responsible for Information Assets? Every information asset must be assigned an **owner**.

Role of Data Owner:

- ❖ Defining the asset
- ❖ Assigning value to the asset
- ❖ Defining the level of protection required
- ❖ Deciding who should have access to the asset
- ❖ Delegating day-to-day security and operational tasks
- ❖ Ongoing governance

What is the Role of the Information Security Officer?

- Accountable for the protection of the information asset.
- Managing the day-to-day controls
- Provide direction and guidance as to the appropriate controls and to ensure that controls are applied consistently throughout the organization
- ISO central repository of security information
- Publishes the classification criteria, maintains the information systems inventories, and implements broad strategic

Why Information Classification required?

The objective of an information classification system is to differentiate data types.

Information Classification: Information classification is the organization of information assets according to their sensitivity to disclosure

Classification Systems: Classification systems are labels that we assign to identify the sensitivity levels

Classification Systems:

- FIPS-99: Sensitivity of the data to be protected
- Government and Military: Based on Executive order of who is handling the data
- Commercial: As per the organization's hierarchy, decided by the information owner

Information Classification based on CIA criteria as:

- Low potential impact: the loss of CIA could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
- Moderate potential impact: the loss of CIA could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- High potential impact: the loss of CIA could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Government & Military Classification Systems

- Top Secret (TS)
- Secret (S)
- Confidential (C)
- Unclassified (U)
- Sensitive But Unclassified (SBU)

Commercial classification systems:

- No standard: Each company can choose its own system that matches its culture and needs
- Usually less complex than the government system

Commercial or private sector classification systems:

- Protected
- Confidential
- Internal Use
- Public

Reclassification/Declassification:

- The need to protect information may change
- With that change, the label assigned to that information may change as well
- The process of downgrading sensitivity levels is called declassification
- The process of upgrading sensitivity levels is called reclassification

Why label required for data classification?

- Labels make it easy to identify the data classification
- Labels can take many forms: electronic, print, audio, and visual.

Why Handling Standards?

- Information needs to be handled in accordance with its classification.
- Handling standards inform custodians and users how to treat the information they use and the systems they interact.

Information Systems Inventory: Many organizations do not have an up-to-date inventory of information systems. This happens for any number of reasons. The most prevalent is a lack of centralized management and control.

What Should Be Inventoried?

- Hardware Assets: Computer equipment, Printers, Communication and networking equipment, etc.
- Software Assets: Operation system software, Productivity software, Application software, etc

CH6:

The Employee Lifecycle:

- Recruitment: It includes all the processes leading up to and including the hiring of a new employee.
- Onboarding: The employee is added to the organization's payroll and benefits systems.
- User provisioning: The employee is assigned equipment as well as physical and technical access permissions.
- Orientation: The employee settles into the job, integrates with the corporate culture, familiarizes himself with coworkers and management, and establishes his role within the organization.
- Career development: The employee matures in his role in the organization. Professional development frequently means a change in roles and responsibilities.
- Termination: The employee leaves the organization.

What is SETA? Security, Education, Training and Awareness

Types of Background Checks:

TABLE 6.1 Types of Background Checks

Check Type	Description
Educational	Verification that all educational credentials listed on the application, resume, or cover letter are valid and have been awarded.
Employment	Verification of all relevant previous employment as listed on the application, resume, or cover letter.
License/certification	Verification of all relevant licenses, certifications, or credentials.
Credit history	Checking the credit history of the selected applicant or employee. Federal laws prohibit discrimination against an applicant or employee because of bankruptcy. Federal law also requires that applicants be notified if their credit history influences the employment decision.
Criminal history	Verification that the selected applicant or employee does not have any undisclosed criminal history.

What Happens in the Onboarding Phase?

- The new hire is added to the organization's payroll and benefit systems
- New employees must provide
  - Proof of identity
  - Work authorization
  - Tax identification

What Should an Employee Learn During Orientation? His responsibilities, Information handling standards and privacy protocols

Components of an Acceptable Use Agreement

• Introduction • Data classifications	• Applicable policy statement • Handling standards	• Contacts • Sanctions for violations	• acknowledgment

Hackers adapt: If it is easier to use social engineering – i.e., targeting users – rather than hack a network device, that is the road they will take

The Importance of Employee Agreements:

Employee Agreements:	Confidentiality or non-disclosure agreements	Acceptable Use Agreement
Defines	Agreement between employees and organization	A policy contract between the company and information systems user
Goal	To protect sensitive information	To ensure that the organization equipment are safe and protected.
Important in Situations	• When an employee is terminated or leaves. • When a third-party contractor was employed	When the organization gave the employee some equipment he has to assign in the acceptable agreement to keep it safe and not to use it for different purpose