2025 CISSP Mentor Program

SESSION 2

Evan Francen

FRSecure

BEFORE WE BEGIN

Some ageless wisdom

Complexity is the **WORST** enemy of information security.

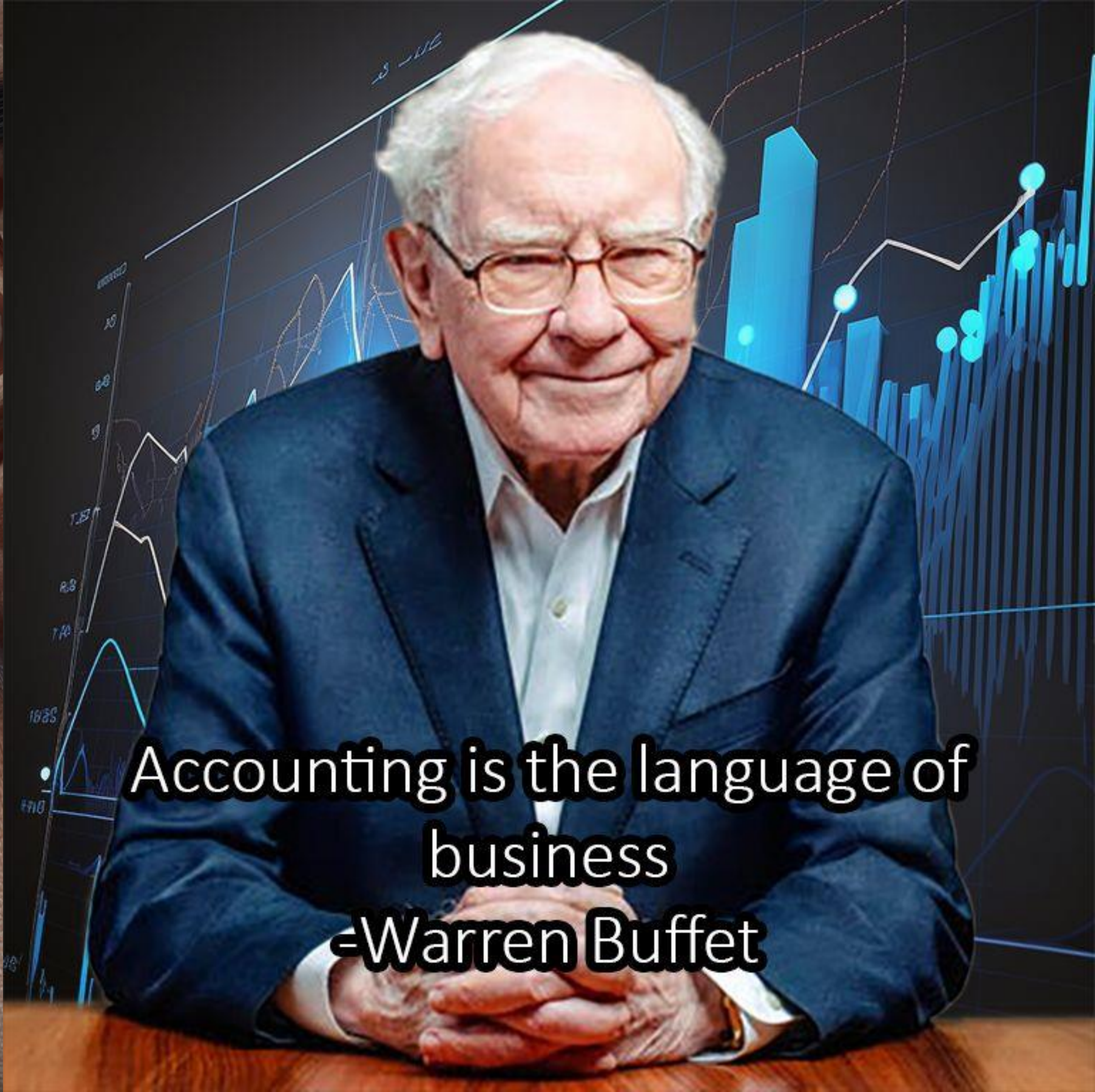
ALWAYS

BEFORE WE BEGIN

Some ageless wisdom (one more)

The language of business is accounting.

NOT cybersecurity



Accounting is the language of business
-Warren Buffet

2025 CISSP MENTOR PROGRAM

AGENDA – SESSION 2

Chapter 1/Chapter 2 (from the book)

Chapter 1 - Security Governance Through Principles and Policies

- Security 101
- Understand and Apply Security Concepts
- Evaluate and Apply Security Governance Principles
- Manage the Security Function
- Security Policy, Standards, Procedures, and Guidelines
- Threat Modeling
- Supply Chain Risk Management

Chapter 2 - Personnel Security and Risk Management Concepts

2025 CISSP MENTOR PROGRAM

AGENDA – SESSION 2

Chapter 1/Chapter 2 (from the book)

Chapter 1 - Security Governance Through Principles and Policies

Chapter 2 - Personnel Security and Risk Management Concepts

- Personnel Security Policies and Procedures
- Understand and Apply Risk Management Concepts
- Social Engineering
- Establish and Maintain a Security Awareness, Education, and Training Program

Pages 1 – 114 in the Kindle version of the book.

NOTE: The book bounces around domains (remember these), we're covering stuff from Domain 1 (Security and Risk Management) and Domain 3 (Security Architecture and Engineering.

221 slides!!!

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Information security is ________________________.

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Information security is **risk management**.

CHAPTER 1

Security Governance Through Principles and Policies

Information security is risk management.

Risk is __________________________.

CHAPTER 1

Security Governance Through Principles and Policies

Information security is **risk management**.

Risk is the **likelihood** of something bad happening and the **impact** if it did.

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Information security is **risk management**.

Risk is the **likelihood** of **something bad** happening and the **impact** if it did.

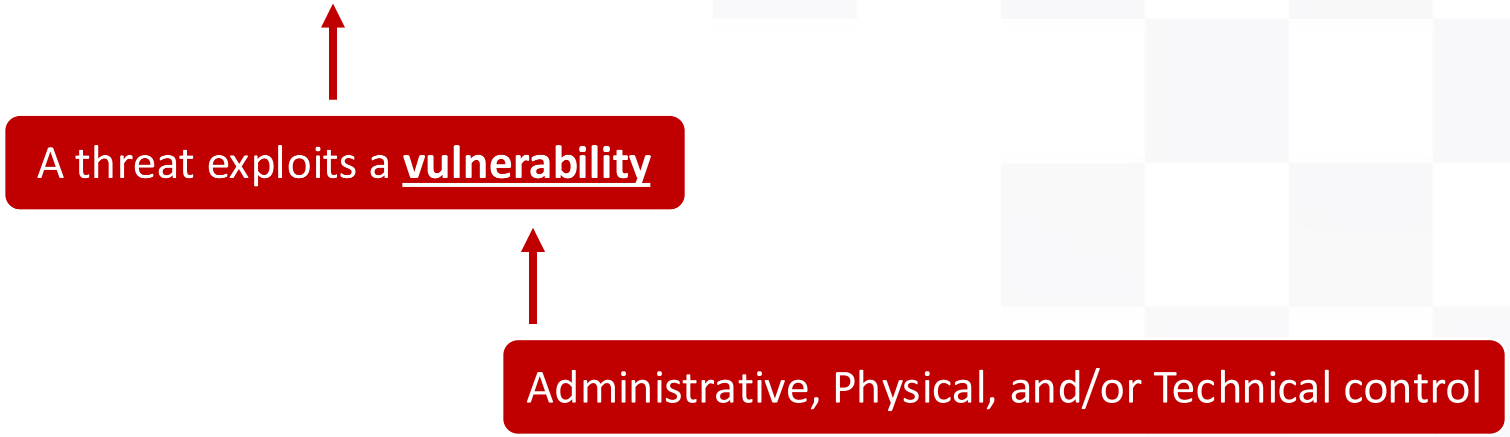
A threat exploits a vulnerability

CHAPTER 1

Security Governance Through Principles and Policies

Information security is risk management.

Risk is the likelihood of something bad happening and the impact if it did.



A threat exploits a **vulnerability**

Administrative, Physical, and/or Technical control

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Information security is **risk management**.

Can’t do this without assessment, decision-making, and implementation.

Risk is the **likelihood** of **something bad** happening and the **impact** if it did.

A threat exploits a **vulnerability**

Administrative, Physical, and/or Technical control

CHAPTER 1

Security Governance Through Principles and Policies

Information security is **risk management**. ←

Can’t do this without assessment, decision-making, and implementation.

Risk is the **likelihood** of **something bad** happening and the **impact** if it did.

A threat exploits a **vulnerability**

Administrative, Physical, and/or Technical control

We’ll come back to this later, but this is **FUNDAMENTAL**.

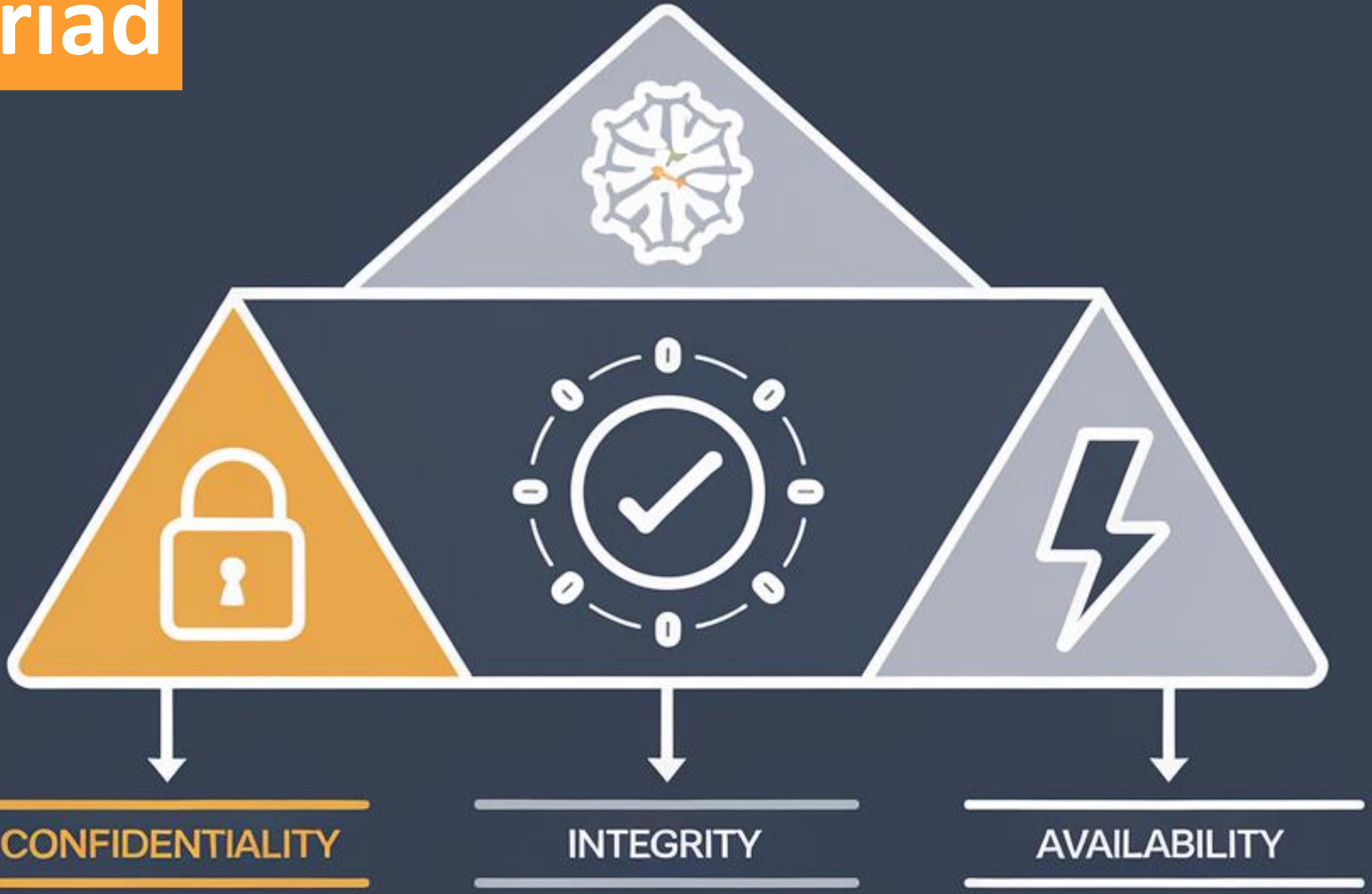
2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

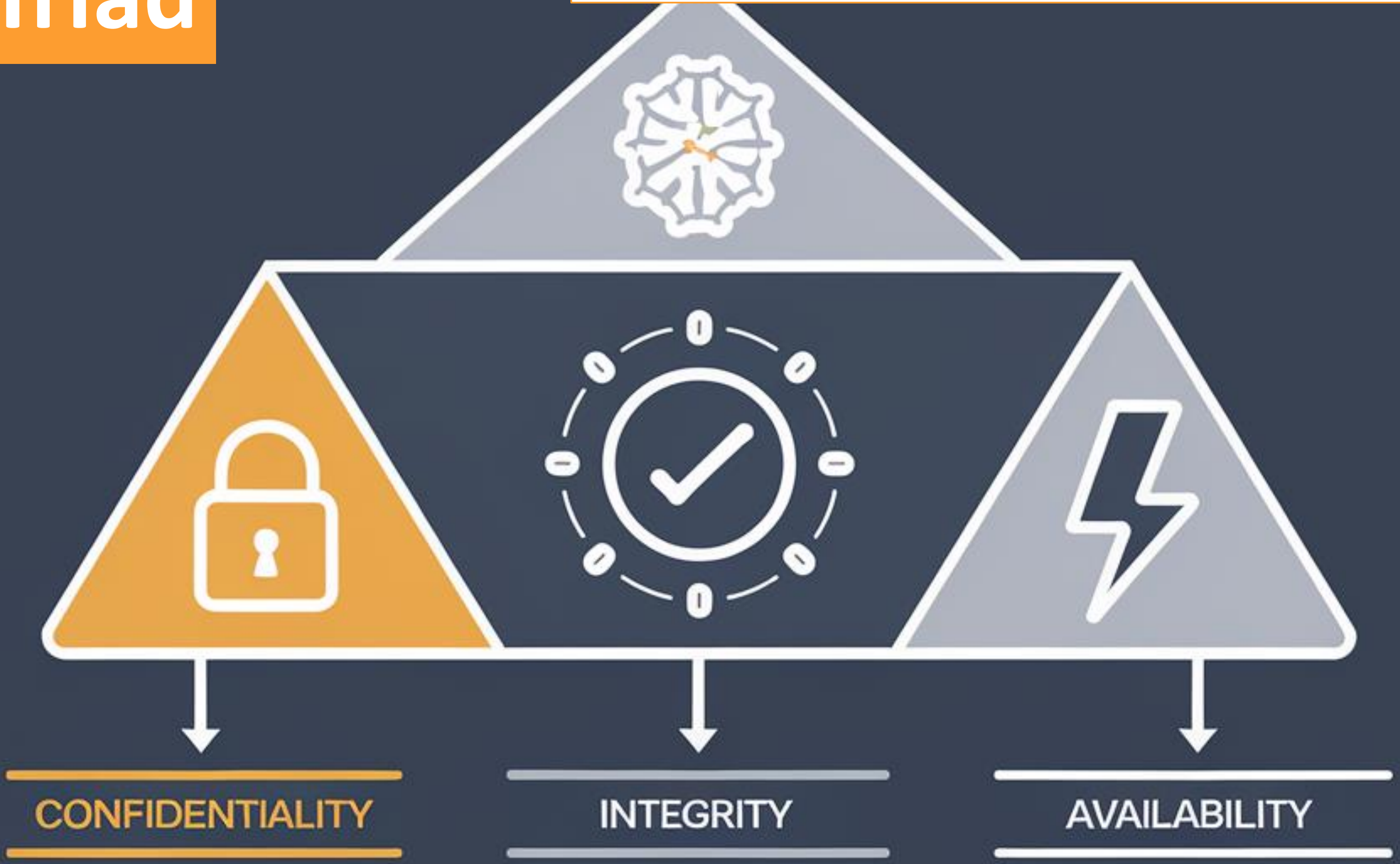
Understand and Apply Security Concepts

CIA Triad



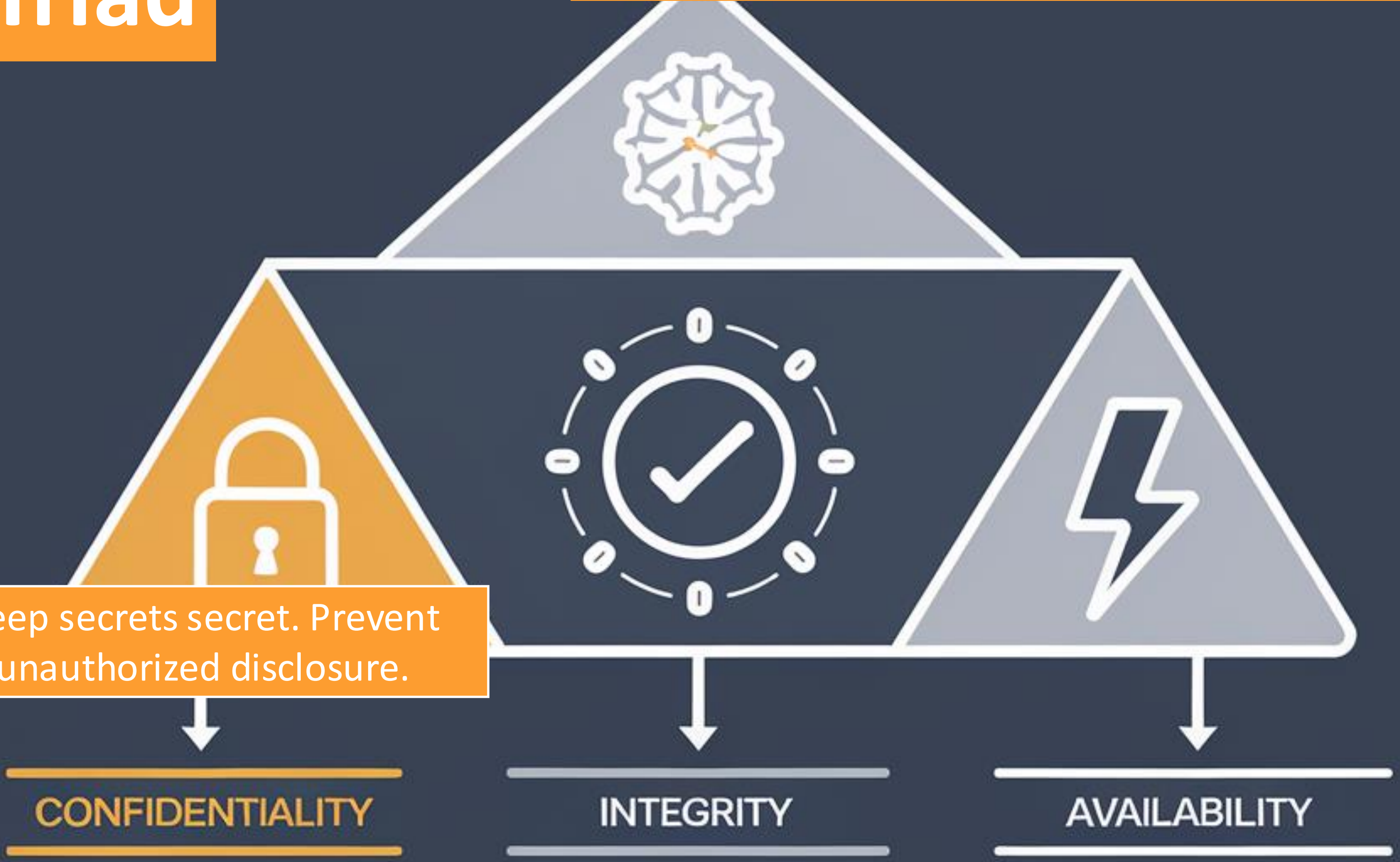
CIA Triad

Somebody thought it was a good idea to add **authenticity**, and **nonrepudiation**, then call it the “*Five Pillars of Information Security*”.



CIA Triad

Somebody thought it was a good idea to add **authenticity**, and **nonrepudiation**, then call it the “*Five Pillars of Information Security*”.



Keep secrets secret. Prevent unauthorized disclosure.

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **CONFIDENTIALITY**:

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **CONFIDENTIALITY**:

- **Sensitivity** - the potential impact or harm that could result from unauthorized disclosure of specific data, based on its importance or confidentiality level.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **CONFIDENTIALITY**:

- **Sensitivity** - the potential impact or harm that could result from unauthorized disclosure of specific data, based on its importance or confidentiality level.
- **Discretion** - refers to the careful judgment and responsibility exercised by individuals in controlling access to sensitive information, ensuring it’s only shared with authorized parties

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **CONFIDENTIALITY**:

- **Sensitivity** - the potential impact or harm that could result from unauthorized disclosure of specific data, based on its importance or confidentiality level.
- **Discretion** - refers to the careful judgment and responsibility exercised by individuals in controlling access to sensitive information, ensuring it’s only shared with authorized parties
- **Concealment** - the deliberate act of hiding or obscuring sensitive information to prevent unauthorized access or disclosure

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **CONFIDENTIALITY**:

- **Sensitivity** - the potential impact or harm that could result from unauthorized disclosure of specific data, based on its importance or confidentiality level.
- **Discretion** - refers to the careful judgment and responsibility exercised by individuals in controlling access to sensitive information, ensuring it's only shared with authorized parties
- **Concealment** - the deliberate act of hiding or obscuring sensitive information to prevent unauthorized access or disclosure
- **Secrecy** - the strict limitation of information access to only those with a clear, authorized need to know, ensuring that the data remains undisclosed to others.

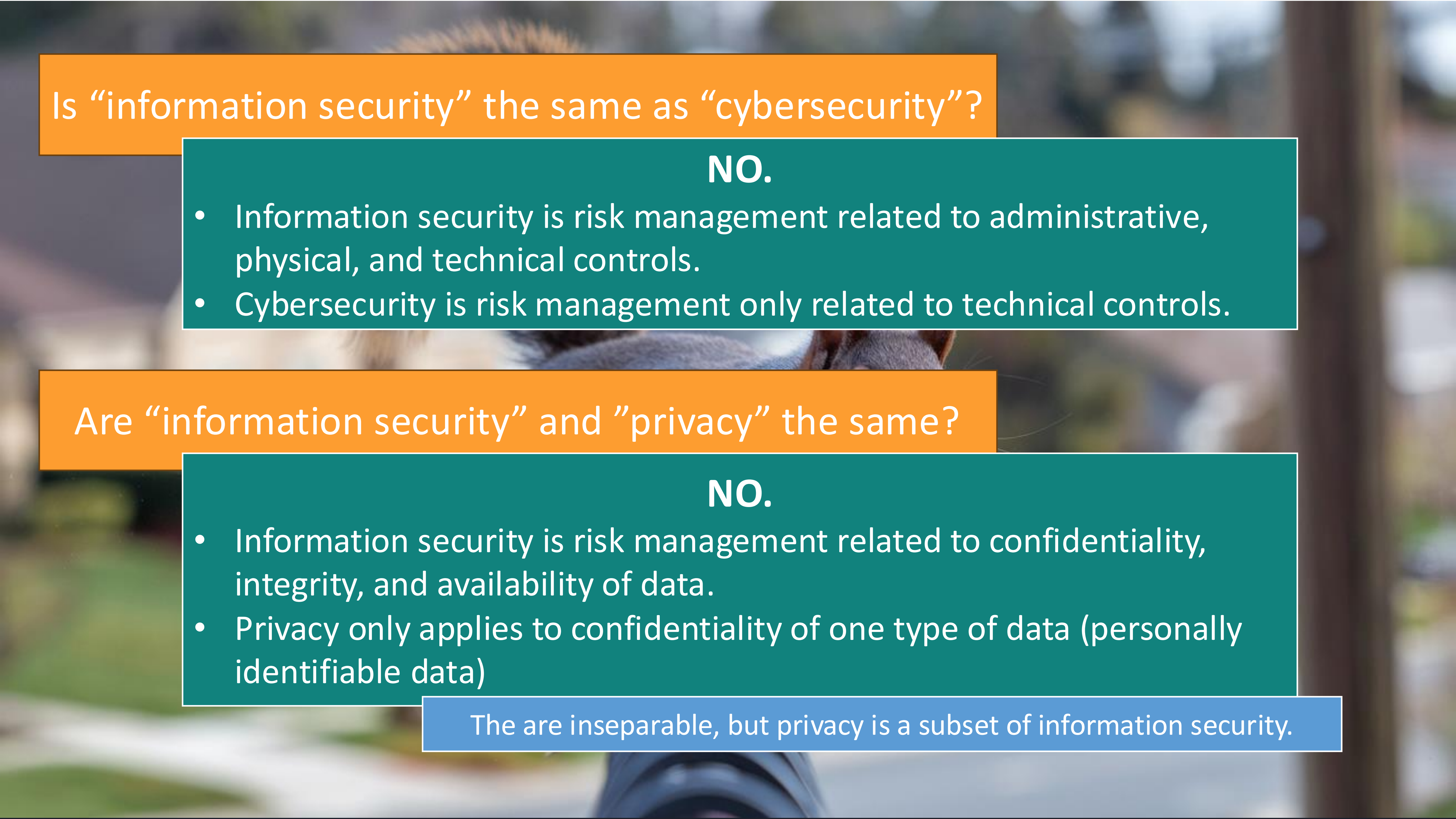
CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **CONFIDENTIALITY**:

- **Sensitivity** - the potential impact or harm that could result from unauthorized disclosure of specific data, based on its importance or confidentiality level.
- **Discretion** - refers to the careful judgment and responsibility exercised by individuals in controlling access to sensitive information, ensuring it's only shared with authorized parties
- **Concealment** - the deliberate act of hiding or obscuring sensitive information to prevent unauthorized access or disclosure
- **Secrecy** - the strict limitation of information access to only those with a clear, authorized need to know, ensuring that the data remains undisclosed to others.
- **Privacy** - the right of individuals to control how their personal information is collected, used, and shared, ensuring it is protected from unauthorized access or exposure.



Is “information security” the same as “cybersecurity”?

NO.

- Information security is risk management related to administrative, physical, and technical controls.
- Cybersecurity is risk management only related to technical controls.

Are “information security” and ”privacy” the same?

NO.

- Information security is risk management related to confidentiality, integrity, and availability of data.
- Privacy only applies to confidentiality of one type of data (personally identifiable data)

The are inseparable, but privacy is a subset of information security.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **CONFIDENTIALITY**:

- **Sensitivity** - the potential impact or harm that could result from unauthorized disclosure of specific data, based on its importance or confidentiality level.
- **Discretion** - refers to the careful judgment and responsibility exercised by individuals in controlling access to sensitive information, ensuring it's only shared with authorized parties
- **Concealment** - the deliberate act of hiding or obscuring sensitive information to prevent unauthorized access or disclosure
- **Secrecy** - the strict limitation of information access to only those with a clear, authorized need to know, ensuring that the data remains undisclosed to others.
- **Privacy** - the right of individuals to control how their personal information is collected, used, and shared, ensuring it is protected from unauthorized access or exposure.
- **Seclusion** - the state of keeping data isolated or separated to minimize exposure and reduce the risk of unauthorized access.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **CONFIDENTIALITY**:

- **Sensitivity** - the potential impact or harm that could result from unauthorized disclosure of specific data, based on its importance or confidentiality level.
- **Discretion** - refers to the careful judgment and responsibility exercised by individuals in controlling access to sensitive information, ensuring it’s only shared with authorized parties
- **Concealment** - the deliberate act of hiding or obscuring sensitive information to prevent unauthorized access or disclosure
- **Secrecy** - the strict limitation of information access to only those with a clear, authorized need to know, ensuring that the data remains undisclosed to others.
- **Privacy** - the right of individuals to control how their personal information is collected, used, and shared, ensuring it is protected from unauthorized access or exposure.
- **Seclusion** - the state of keeping data isolated or separated to minimize exposure and reduce the risk of unauthorized access.
- **Isolation** - the practice of segregating systems, processes, or data to prevent unauthorized access and limit the spread of potential breaches.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **CONFIDENTIALITY**:

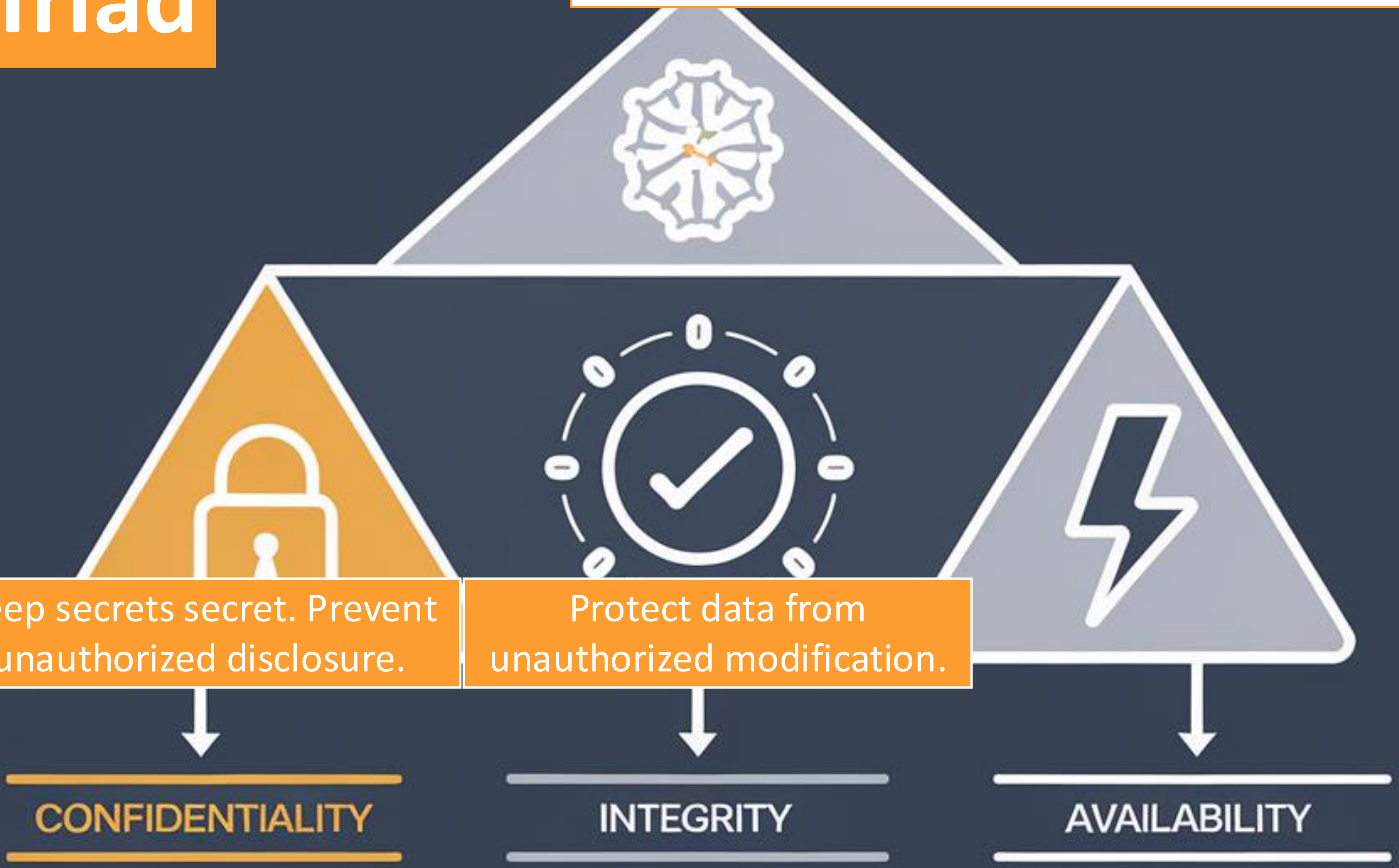
- **Sensitivity** - the potential impact or harm that could result data, based on its importance or confidentiality level.
- **Discretion** - refers to the careful judgment and responsibili access to sensitive information, ensuring it's only shared w
- **Concealment** - the deliberate act of hiding or obscuring sensitive information to prevent unauthorized access or disclosure
- **Secrecy** - the strict limitation of information access to only those with a clear, authorized need to know, ensuring that the data remains undisclosed to others.
- **Privacy** - the right of individuals to control how their personal information is collected, used, and shared, ensuring it is protected from unauthorized access or exposure.
- **Seclusion** - the state of keeping data isolated or separated to minimize exposure and reduce the risk of unauthorized access.
- **Isolation** - the practice of segregating systems, processes, or data to prevent unauthorized access and limit the spread of potential breaches.

Up for a challenge?!

Find (or create) an example of each of these.

CIA Triad

Somebody thought it was a good idea to add **authenticity**, and **nonrepudiation**, then call it the “*Five Pillars of Information Security*”.



Keep secrets secret. Prevent unauthorized disclosure.

Protect data from unauthorized modification.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **INTEGRITY**:

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **INTEGRITY**:

- **Accuracy** - the correctness and precision of data, ensuring it reflects the real-world values or events it is intended to represent without error or distortion.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **INTEGRITY**:

- **Accuracy** - the correctness and precision of data, ensuring it reflects the real-world values or events it is intended to represent without error or distortion.
- **Truthfulness** - the assurance that data is genuine, authentic, and has not been falsified or misleadingly altered.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **INTEGRITY**:

- **Accuracy** - the correctness and precision of data, ensuring it reflects the real-world values or events it is intended to represent without error or distortion.
- **Truthfulness** - the assurance that data is genuine, authentic, and has not been falsified or misleadingly altered.
- **Validity** - the extent to which data is logically sound, conforms to defined formats or rules, and is appropriate for its intended purpose.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **INTEGRITY**:

- **Accuracy** - the correctness and precision of data, ensuring it reflects the real-world values or events it is intended to represent without error or distortion.
- **Truthfulness** - the assurance that data is genuine, authentic, and has not been falsified or misleadingly altered.
- **Validity** - the extent to which data is logically sound, conforms to defined formats or rules, and is appropriate for its intended purpose.
- **Accountability** - the ability to trace actions and changes to data back to specific individuals or systems, ensuring responsibility for maintaining its accuracy and trustworthiness.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **INTEGRITY**:

- **Accuracy** - the correctness and precision of data, ensuring it reflects the real-world values or events it is intended to represent without error or distortion.
- **Truthfulness** - the assurance that data is genuine, authentic, and has not been falsified or misleadingly altered.
- **Validity** - the extent to which data is logically sound, conforms to defined formats or rules, and is appropriate for its intended purpose.
- **Accountability** - the ability to trace actions and changes to data back to specific individuals or systems, ensuring responsibility for maintaining its accuracy and trustworthiness.
- **Responsibility** - the obligation of individuals or entities to ensure that data is accurate, complete, and protected from unauthorized modification or corruption.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **INTEGRITY**:

- **Accuracy** - the correctness and precision of data, ensuring it reflects the real-world values or events it is intended to represent without error or distortion.
- **Truthfulness** - the assurance that data is genuine, authentic, and has not been falsified or misleadingly altered.
- **Validity** - the extent to which data is logically sound, conforms to defined formats or rules, and is appropriate for its intended purpose.
- **Accountability** - the ability to trace actions and changes to data back to specific individuals or systems, ensuring responsibility for maintaining its accuracy and trustworthiness.
- **Responsibility** - the obligation of individuals or entities to ensure that data is accurate, complete, and protected from unauthorized modification or corruption.
- **Completeness** - the assurance that all required data is present, with nothing missing or omitted, to fully represent the intended information or process.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **INTEGRITY**:

- **Accuracy** - the correctness and precision of data, ensuring it reflects the real-world values or events it is intended to represent without error or distortion.
- **Truthfulness** - the assurance that data is genuine, authentic, and has not been falsified or misleadingly altered.
- **Validity** - the extent to which data is logically sound, conforms to defined formats or rules, and is appropriate for its intended purpose.
- **Accountability** - the ability to trace actions and changes to data back to specific individuals or systems, ensuring responsibility for maintaining its accuracy and trustworthiness.
- **Responsibility** - the obligation of individuals or entities to ensure that data is accurate, complete, and protected from unauthorized modification or corruption.
- **Completeness** - the assurance that all required data is present, with nothing missing or omitted, to fully represent the intended information or process.
- **Comprehensiveness** - the extent to which data captures the full scope of necessary information, covering all relevant aspects without gaps or exclusions.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **INTEGRITY**:

- **Accuracy** - the correctness and precision of data, ensuring it reflects the real-world values or events it is intended to represent without error or distortion.
- **Truthfulness** - the assurance that data is genuine, authentic, and has not been falsified or misleadingly altered.

This is authenticity

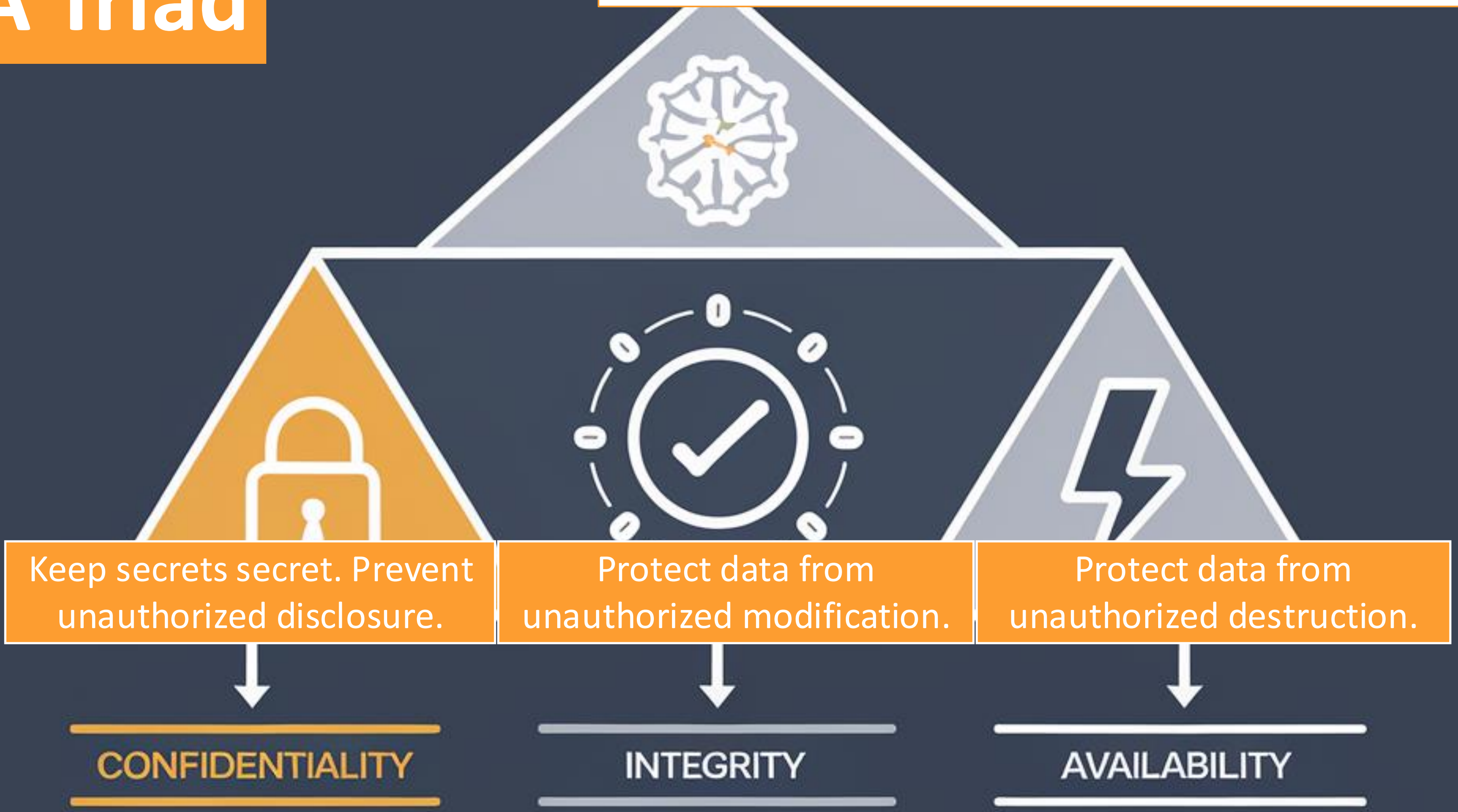
- **Validity** - the extent to which data is logically sound, conforms to defined formats or rules, and is appropriate for its intended purpose.
- **Accountability** - the ability to trace actions and changes to data back to specific individuals or systems, ensuring responsibility for maintaining its accuracy and trustworthiness.

This is nonrepudiation

- **Responsibility** - the obligation of individuals or entities to ensure that data is accurate, complete, and protected from unauthorized modification or corruption.
- **Completeness** - the assurance that all required data is present, with nothing missing or omitted, to fully represent the intended information or process.
- **Comprehensiveness** - the extent to which data captures the full scope of necessary information, covering all relevant aspects without gaps or exclusions.

CIA Triad

Somebody thought it was a good idea to add **authenticity**, and **nonrepudiation**, then call it the "*Five Pillars of Information Security*".



Keep secrets secret. Prevent unauthorized disclosure.

Protect data from unauthorized modification.

Protect data from unauthorized destruction.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **AVAILABILITY**:

- **Usability** - the extent to which data is accessible, functional, and in a format that allows authorized users to effectively retrieve and utilize it when needed.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Things related to **AVAILABILITY**:

- **Usability** - the extent to which data is accessible, functional, and in a format that allows authorized users to effectively retrieve and utilize it when needed.
- **Accessibility** - the ability of authorized users to reliably retrieve and use data when needed, without unnecessary barriers or delays.

CHAPTER 1

Security Governance Through Principles and Policies

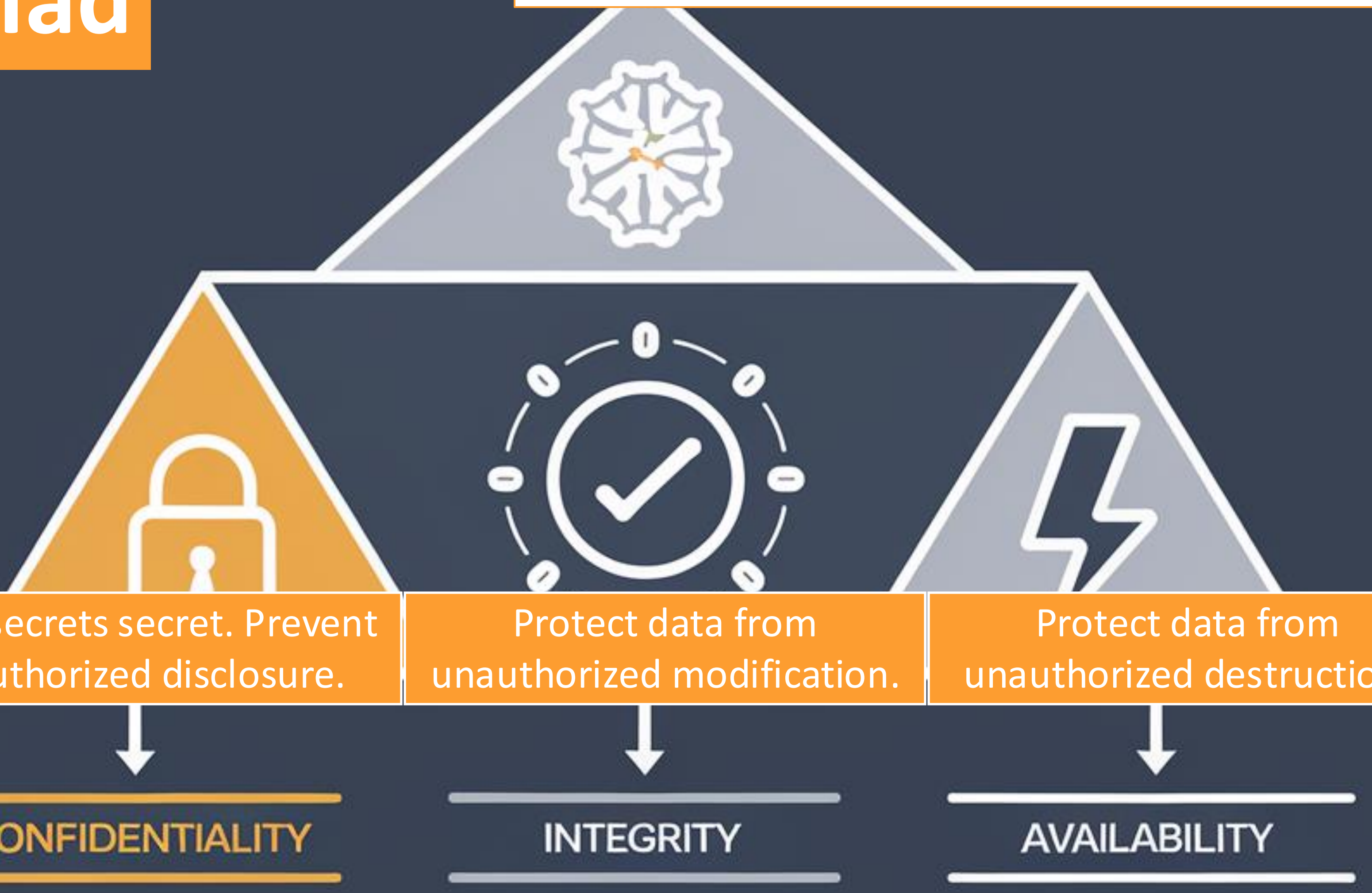
Understand and Apply Security Concepts

Things related to **AVAILABILITY**:

- **Usability** - the extent to which data is accessible, functional, and in a format that allows authorized users to effectively retrieve and utilize it when needed.
- **Accessibility** - the ability of authorized users to reliably retrieve and use data when needed, without unnecessary barriers or delays.
- **Timeliness** - the assurance that data is accessible and up-to-date at the exact moment it is needed to support decision-making or operations.

CIA Triad

Somebody thought it was a good idea to add **authenticity**, and **nonrepudiation**, then call it the "*Five Pillars of Information Security*".

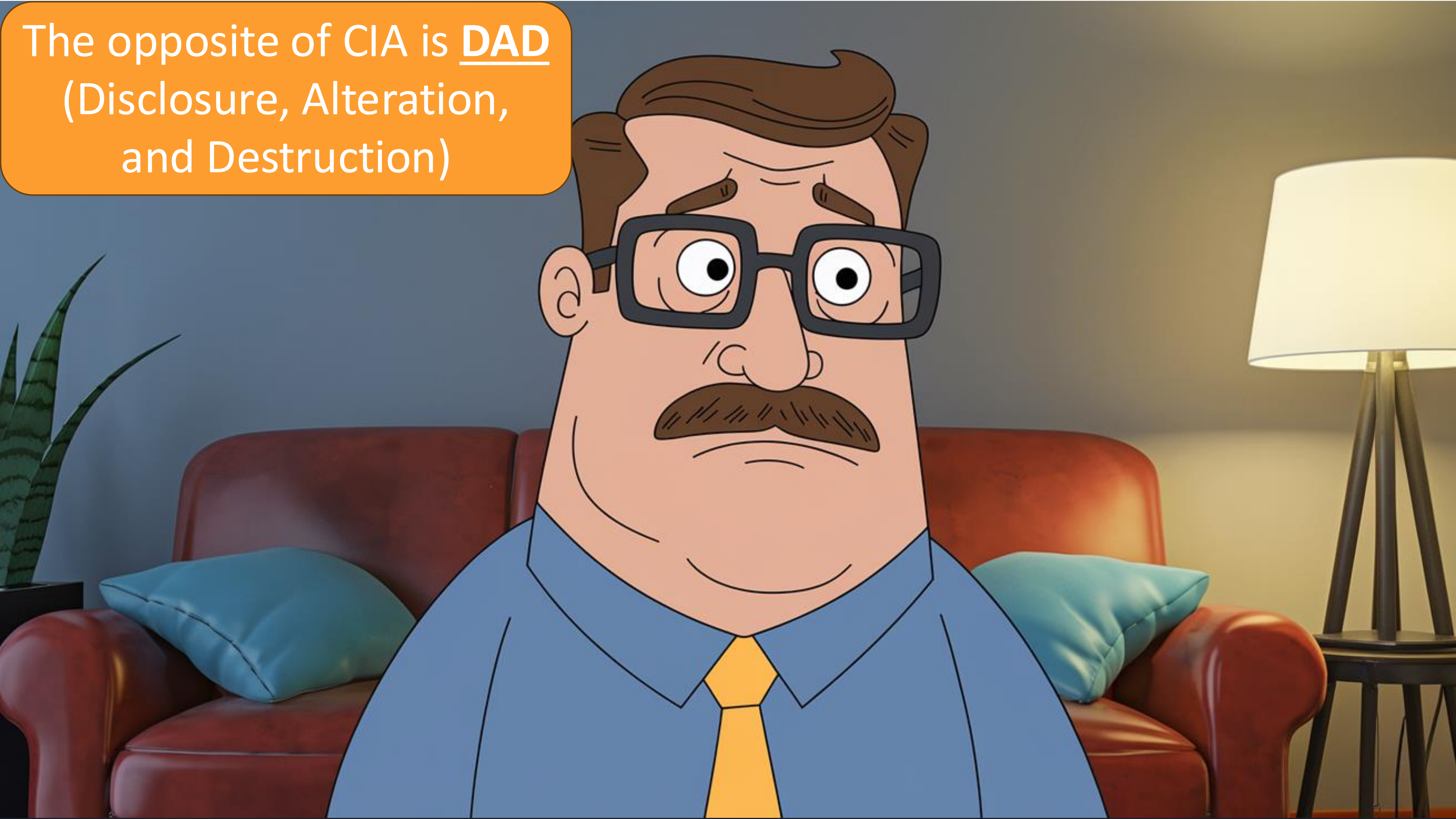


Keep secrets secret. Prevent unauthorized disclosure.

Protect data from unauthorized modification.

Protect data from unauthorized destruction.

The opposite of CIA is **DAD** (Disclosure, Alteration, and Destruction)



The opposite of CIA is **DAD** (Disclosure, Alteration, and Destruction)

Why did the computer go to therapy after getting hacked?

Because it had too many trust issues!

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

There's more!

CHAPTER 1

Security Governance Through Principles and Policies

There's more!

Understand and Apply Security Concepts

- **Authenticity** - the assurance that data, systems, or users are genuine and trustworthy, verifying that they are exactly who or what they claim to be. It helps prevent impersonation, tampering, or unauthorized access.

CHAPTER 1

Security Governance Through Principles and Policies

There's more!

Understand and Apply Security Concepts

- **Authenticity** - the assurance that data, systems, or users are genuine and trustworthy, verifying that they are exactly who or what they claim to be. It helps prevent impersonation, tampering, or unauthorized access.
- **Nonrepudiation** - the assurance that a party in a communication or transaction cannot deny the authenticity of their signature, message, or action. It provides proof of origin and integrity, often using digital signatures and audit trails.

Example Scenario:

A company's CFO digitally signs a financial transfer request to move $500,000 to a vendor. Later, when the funds are transferred, the CFO claims they never approved the transaction. However, the system uses digital signatures and audit logs to verify the request came from the CFO's secure credentials and was timestamped at the exact time their account was used. Because of nonrepudiation, the company can prove the action was authorized by the CFO, preventing fraud, ensuring accountability, and protecting the integrity of financial operations.

CHAPTER 1

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

There's more!

It says AAA, but there's four As and an I!

Together, these things are often called "Access Control".

CHAPTER 1

Security Governance Through Principles and Policies

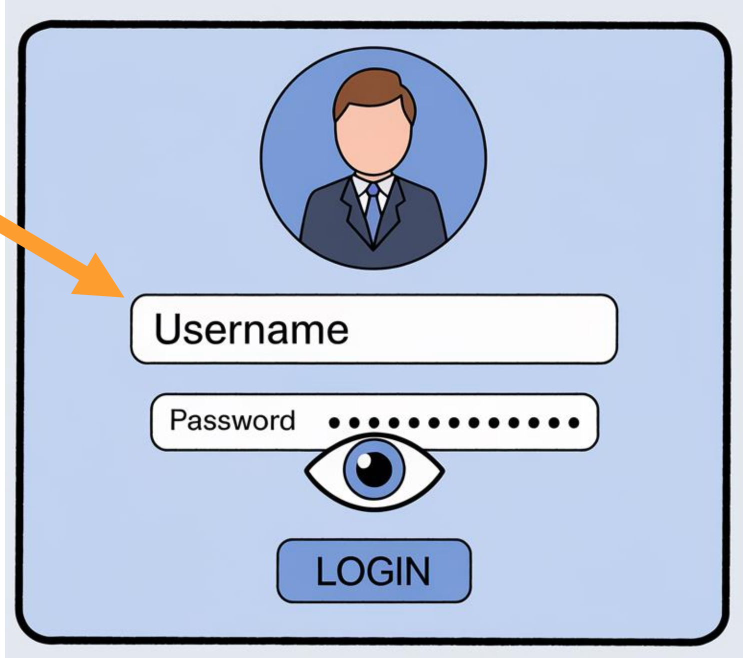
There’s more!

Understand and Apply Security Concepts

It says AAA, but there’s four As and an I!

Together, these things are often called “Access Control”:

- **Identification** - the process of claiming or declaring a unique identity, such as a username or ID, to access a system or resource.



CHAPTER 1

Security Governance Through Principles and Policies

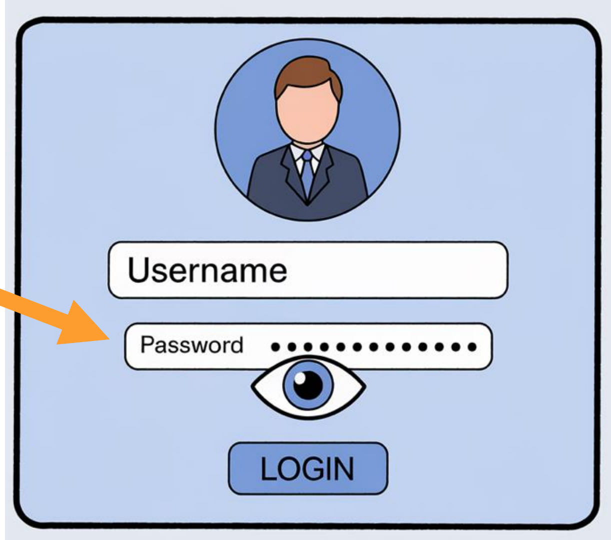
There's more!

Understand and Apply Security Concepts

It says AAA, but there's four As and an I!

Together, these things are often called "Access Control":

- **Identification** - the process of claiming or declaring a unique identity, such as a username or ID, to access a system or resource.
- **Authentication** - the process of verifying (or proving) that a claimed identity is valid, typically through credentials like passwords, biometrics, or security tokens.



CHAPTER 1

Security Governance Through Principles and Policies

There's more!

Understand and Apply Security Concepts

It says AAA, but there's four As and an I!

Together, these things are often called "Access Control":

Assuming these worked

- **Identification** - the process of claiming or declaring a unique identity, such as a username or ID, to access a system or resource.
- **Authentication** - the process of verifying (or proving) that a claimed identity is valid, typically through credentials like passwords, biometrics, or security tokens.

CHAPTER 1

There's more!

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

It says AAA, but there's four As and an I!

Together, these things are often called "Access Control":

- **Identification** - the process of claiming or declaring a unique identity, such as a username or ID, to access a system or resource.
- **Authentication** - the process of verifying (or proving) that a claimed identity is valid, typically through credentials like passwords, biometrics, or security tokens.
- **Authorization** - the process of granting or denying a verified user permission to access specific resources or perform certain actions based on predefined policies.

CHAPTER 1

Security Governance Through Principles and Policies

There's more!

Understand and Apply Security Concepts

It says AAA, but there's four As and an I!

Together, these things are often called "Access Control":

- **Identification** - the process of claiming or declaring a unique identity, such as a username or ID, to access a system or resource.
- **Authentication** - the process of verifying (or proving) that a claimed identity is valid, typically through credentials like passwords, biometrics, or security tokens.
- **Authorization** - the process of granting or denying a verified user permission to access specific resources or perform certain actions based on predefined policies.
- **Auditing** - the process of recording and examining system activities and access events to ensure compliance, detect anomalies, and support accountability.

CHAPTER 1

Security Governance Through Principles and Policies

There’s more!

Understand and Apply Security Concepts

It says AAA, but there’s four As and an I!

Together, these things are often called “Access Control”:

- **Identification** - the process of claiming or declaring a unique identity, such as a username or ID, to access a system or resource.
- **Authentication** - the process of verifying (or proving) that a claimed identity is valid, typically through credentials like passwords, biometrics, or security tokens.
- **Authorization** - the process of granting or denying a verified user permission to access specific resources or perform certain actions based on predefined policies.
- **Auditing** - the process of recording and examining system activities and access events to ensure compliance, detect anomalies, and support accountability.
- **Accounting** - the tracking and reporting of user activities and resource usage to support auditing, billing, and accountability.

CHAPTER 1

There's more!

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Still going… Not specific to access control now.

- **Defense in Depth** - the strategic use of multiple, layered security measures to protect data and systems, ensuring that if one control fails, others still provide protection.

There's more!

Practical Example of Defense in Depth:

A company secures its internal network using multiple layers: a firewall to block unauthorized traffic, multi-factor authentication (MFA) for user logins, endpoint protection software on all devices, network segmentation to isolate sensitive systems, and continuous logging and monitoring for anomalies.

Pros:

- Redundancy: If one layer fails (e.g., a user falls for a phishing attack), other controls like MFA or endpoint detection can still prevent or mitigate the breach.
- Reduced Risk: It makes successful attacks more difficult, requiring attackers to bypass several independent defenses.
- Comprehensive Coverage: Addresses multiple types of threats—technical, physical, and human.

Cons:

- **Complexity**: Managing and maintaining multiple overlapping controls can increase administrative overhead and potential for misconfiguration.
- Cost: More tools, licenses, and personnel are needed, which can strain smaller organizations' budgets.
- User Frustration: Layered security (e.g., frequent MFA prompts, limited access) can lead to productivity complaints or attempts to bypass controls.

CHAPTER 1

Security Governance Through Principles and Policies

There's more!

Understand and Apply Security Concepts

Still going… Not specific to access control now.

- **Defense in Depth** - the strategic use of multiple, layered security measures to protect data and systems, ensuring that if one control fails, others still provide protection.
- **Abstraction** - the process of hiding complex implementation details and exposing only essential features to reduce risk, simplify access control, and minimize the attack surface.

CHAPTER 1

There's more!

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Still going… Not specific to access control now.

- **Defense in Depth** - the strategic use of multiple, layered security measures to protect data and systems, ensuring that if one control fails, others still provide protection.
- **Abstraction** - the process of hiding complex implementation details and exposing only essential features to reduce risk, simplify access control, and minimize the attack surface.
- **Data hiding** - the practice of concealing internal data structures or sensitive information from unauthorized users to prevent accidental or malicious access or modification.

CHAPTER 1

There's more!

Security Governance Through Principles and Policies

Understand and Apply Security Concepts

Still going… Not specific to access control now.

- **Defense in Depth** - the strategic use of multiple, layered security measures to protect data and systems, ensuring that if one control fails, others still provide protection.
- **Abstraction** - the process of hiding complex implementation details and exposing only essential features to reduce risk, simplify access control, and minimize the attack surface.
- **Data hiding** - the practice of concealing internal data structures or sensitive information from unauthorized users to prevent accidental or malicious access or modification.
- **Encryption** - the process of converting readable data into an unreadable format using an algorithm and key, ensuring that only authorized parties can access the original information.

CHAPTER 1

Security Governance Through Principles and Policies

There's more!

Understand and Apply Security Concepts

Still going… Not specific to access control now.

- **Defense in Depth** - the strategic use of multiple, layered security measures to protect data and systems, ensuring that if one control fails, others still provide protection.
- **Abstraction** - the process of hiding complex implementation details and exposing only essential features to reduce risk, simplify access control, and minimize the attack surface.
- **Data hiding** - the practice of concealing internal data structures or sensitive information from unauthorized users to prevent accidental or malicious access or modification.
- **Encryption** - the process of converting readable data into an unreadable format using an algorithm and key, ensuring that only authorized parties can access the original information.

Having fun yet?!

All these fundamental concepts will be expanded upon later. ☺

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Security Boundaries

CHAPTER 1

Security Governance Through Principles and Policies

Security Boundaries

Clearly defined borders—**physical**, **logical**, or **administrative**—that separate different levels of trust, control, or security within or between systems, helping to enforce access controls, contain threats, and protect sensitive resources.

CHAPTER 1

Security Governance Through Principles and Policies

Security Boundaries

Clearly defined borders—**physical**, **logical**, or **administrative**—that separate different levels of trust, control, or security within or between systems, helping to enforce access controls, contain threats, and protect sensitive resources.

Physical Security Boundary:
A locked server room with keycard access that physically restricts who can get close to critical infrastructure like servers, switches, or firewalls.

Logical Security Boundary:
A network firewall that separates an internal trusted network from an untrusted external network (e.g., the internet), enforcing rules about what data can pass between them.

Administrative Security Boundary:
A set of policies and user roles that limits access to HR data to only HR personnel, even though the data resides on the same server used by other departments.

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Evaluate and Apply Security Governance Principles

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Evaluate and Apply Security Governance Principles

- **Security governance** - the framework of policies, processes, and controls that ensure an organization’s information security strategy aligns with its business objectives, complies with regulations, and manages risk effectively.

CHAPTER 1

Security Governance Through Principles and Policies

Evaluate and Apply Security Governance Principles

Governance = Rules for the game.

- **Security governance** - the framework of policies, processes, and controls that ensure an organization's information security strategy aligns with its business objectives, complies with regulations, and manages risk effectively.

CHAPTER 1

Security Governance Through Principles and Policies

Evaluate and Apply Security Governance Principles

Governance = Rules for the game.

- **Security governance** - the framework of policies, processes, and controls that ensure an organization's information security strategy aligns with its business objectives, complies with regulations, and manages risk effectively.
- **Third-party governance** - the processes and controls an organization uses to manage and monitor the security practices of external vendors, partners, or service providers to ensure they meet required security standards and do not introduce undue risk.

CHAPTER 1

Security Governance Through Principles and Policies

Evaluate and Apply Security Governance Principles

Governance = Rules for the game.

- **Security governance** - the framework of policies, processes, and controls that ensure an organization's information security strategy aligns with its business objectives, complies with regulations, and manages risk effectively.
- **Third-party governance** - the processes and controls an organization uses to manage and monitor the security practices of external vendors, partners, or service providers to ensure they meet required security standards and do not introduce undue risk.
    - **Ponemon Institute**'s 2023 report on third-party risk found that **51% of organizations** experienced a data breach caused by a third party.
    - **Gartner** has reported that **60% of organizations** work with over 1,000 third parties and that **cyber incidents involving third parties are growing year over year**.
    - The **IBM Cost of a Data Breach Report 2023** notes that breaches involving third parties cost more and take longer to identify and contain than internal incidents.

CHAPTER 1

Security Governance Through Principles and Policies

Evaluate and Apply Security Governance Principles

Governance = Rules for the game.

- **Security governance** - the framework of policies, processes, and controls that ensure an organization's information security strategy aligns with its business objectives, complies with regulations, and manages risk effectively.
- **Third-party governance** - the processes and controls an organization uses to manage and monitor the security practices of external vendors, partners, or service providers to ensure they meet required security standards and do not introduce undue risk.
  - **Ponemon Institute**'s 2023 report on third-party risk found that **51% of organizations** experienced a data breach caused by a third party.
  - **Gartner** has reported that **60% of organizations** work with over 1,000 third parties and that **cyber incidents involving third parties are growing year over year**.
  - The **IBM Cost of a Data Breach Report 2023** notes that breaches involving third parties cost more and take longer to identify and contain than internal incidents.
- **Documentation review** - the systematic examination of policies, procedures, standards, and records to ensure they are accurate, complete, up to date, and aligned with security requirements, best practices, and compliance obligations.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Security function - the organizational role or team responsible for developing, implementing, managing, and monitoring the strategies, policies, and controls that protect information assets from threats and ensure confidentiality, integrity, and availability.

If information security is risk management (it is), then risk **assessment**(s), **measurement**, risk **decision-making**, and ongoing **improvements** are all imperative.

Great, but who is ultimately responsible for information security within an organization?

I'll give you the answer in the Live Session!

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives

This is **CRITICAL**!

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

This is **CRITICAL**!

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives

- But sadly, it’s not well done in practice in most places. I guess this is opportunity (maybe).

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives

This is **CRITICAL**!

- But sadly, it’s not well done in practice in most places. I guess this is opportunity (maybe).
- The rules for the information security ”game” must be documented, and they’re first documented in **policy**.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives

This is **CRITICAL**!

- But sadly, it’s not well done in practice in most places. I guess this is opportunity (maybe).
- The rules for the information security ”game” must be documented, and they’re first documented in **policy**.
- Do the rules for the game further the business strategy, goals, mission, and objectives **OR** do they hinder them?

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives

This is **CRITICAL**!

- But sadly, it's not well done in practice in most places. I guess this is opportunity (maybe).
- The rules for the information security "game" must be documented, and they're first documented in **policy**.
- Do the rules for the game further the business strategy, goals, mission, and objectives **OR** do they hinder them?
- **Business case** - a structured justification for a security initiative or investment, demonstrating how it supports organizational objectives, mitigates risk, ensures compliance, and delivers **value**—often by weighing costs, benefits, and potential impacts.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives

This is **CRITICAL**!

- But sadly, it's not well done in practice in most places. I guess this is opportunity (maybe).
- The rules for the information security "game" must be documented, and they're first documented in **policy**.
- Do the rules for the game further the business strategy, goals, mission, and objectives **OR** do they hinder them?
- **Business case** - a structured justification for a security initiative or investment, demonstrating how it supports organizational objectives, mitigates risk, ensures compliance, and delivers **value**—often by weighing costs, benefits, and potential impacts.
- **Top-down approach** - a management-driven strategy where senior leadership defines security policies, goals, and priorities, ensuring alignment with business objectives and enabling effective implementation across the organization.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives

This is **CRITICAL**!

- But sadly, it's not well done in practice in most places. I guess this is opportunity (maybe).
- The rules for the information security "game" must be documented, and they're first documented in **policy**.
- Do the rules for the game further the business strategy, goals, mission, and objectives **OR** do they hinder them?
- **Business case** - a structured justification for a security initiative or investment, demonstrating how it supports organizational objectives, mitigates risk, ensures compliance, and delivers value—often by weighing costs, benefits, and potential impacts.
- **Top-down approach** - a management-driven strategy where senior leadership defines security policies, goals, and priorities, ensuring alignment with business objectives and enabling effective implementation across the organization.
- **Bottom-up approach** - a strategy where technical staff or operational teams initiate and implement security measures without formal direction from upper management, often resulting in ad hoc solutions that may lack alignment with broader organizational goals.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives

Documented plans are important for several reasons. Three types of plans covered in the book:

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives

Documented plans are important for several reasons. Three types of plans covered in the book:

1. **Strategic Plan** - outlines the long-term direction and goals of the information security program, typically covering a multi-year horizon (e.g., 3–5 years). It aligns security initiatives with the organization's overall business objectives and risk appetite.

Key Characteristics:

- High-level and broad in scope
- Developed and owned by senior leadership (CISO, CIO)
- Often includes a security mission, vision, and strategic objectives
- Addresses regulatory requirements, emerging risks, and future tech trends

How You'd Use It:
Use this to set the vision and direction for your entire security program. It's your north star—used to justify budgets, guide major initiatives, and align security with business priorities.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives

Documented plans are important for several reasons. Three types of plans covered in the book:

2. **Tactical Plan** - translates the strategic plan into mid-term objectives and actionable projects, typically covering a 1–2-year timeframe. It outlines how strategic goals will be achieved with specific initiatives, tools, and resources.

Key Characteristics:

- Medium-level detail
- Managed by security managers or team leads
- Includes specific projects (e.g., implementing MFA, improving third-party risk)
- Allocates resources and timelines for achieving goals

How You'd Use It:
Use this to plan and manage your initiatives, like building a security awareness program or deploying new technologies. It bridges the gap between high-level vision and day-to-day execution.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives

Documented plans are important for several reasons. Three types of plans covered in the book:

3. **Operational Plan** - a short-term, highly detailed guide that defines the daily, weekly, or monthly tasks required to run and maintain the security program.

Key Characteristics:

- Task-oriented and time-specific
- Includes playbooks, procedures, and runbooks
- Often tied to specific roles or functions (e.g., SOC operations, patch management)
- Owned by technical teams, analysts, or administrators

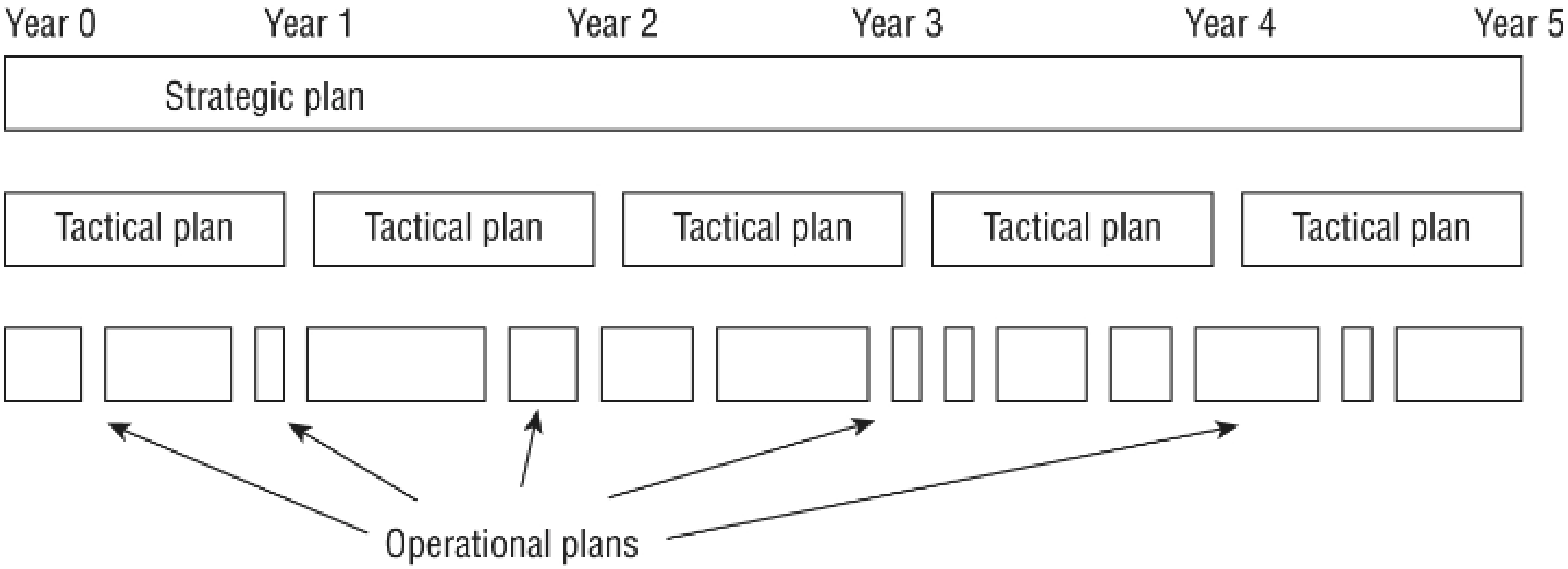
How You'd Use It:
Use this to execute specific tasks, respond to incidents, monitor systems, or maintain compliance. It's where the real boots-on-the-ground work gets done.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives



CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Organizational Roles and Responsibilities

No two organizations are exactly the same.

CHAPTER 1

Security Governance Through Principles and Policies

No two organizations are exactly the same.

Manage the Security Function

Organizational Roles and Responsibilities

Six primary security roles defined by ISC2 are **Senior Manager**, **Security Professional**, **Asset Owner**, **Custodian**, **User**, and **Auditor**.

Other more formal roles may include…

CHAPTER 1

Security Governance Through Principles and Policies

No two organizations are exactly the same.

Manage the Security Function

Organizational Roles and Responsibilities

Executive & Leadership Roles

- Chief Information Security Officer (CISO)
  - Sets the overall security strategy and direction.
  - Aligns security with business goals.
  - Reports to executive leadership or the board.
- Deputy CISO / Security Director
  - Assists the CISO, often managing day-to-day operations.
  - Coordinates between teams and oversees program execution.

CHAPTER 1

Security Governance Through Principles and Policies

No two organizations are exactly the same.

Manage the Security Function

Organizational Roles and Responsibilities

Management & Oversight Roles

- Security Program Manager
  - Oversees large-scale security initiatives and project portfolios.
  - Ensures milestones, budgets, and timelines are met.
- Compliance / GRC Manager
  - Manages governance, risk, and compliance (GRC) functions.
  - Oversees regulatory compliance and policy frameworks (e.g., ISO 27001, NIST, HIPAA).
- Security Awareness & Training Lead
  - Develops and delivers security education to employees.
  - Promotes a security-conscious culture.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Organizational Roles and Responsibilities

Technical & Operational Roles

- **Security Architect**
  - Designs secure systems, networks, and cloud environments.
  - Ensures security is built into infrastructure and software.
- **Security Engineer**
  - Implements and manages technical security controls (e.g., firewalls, SIEMs, EDR).
  - Builds automation and tooling for defense.
- **Security Analyst**
  - Monitors systems for threats, analyzes alerts, and investigates incidents.
  - Often part of the SOC (Security Operations Center)
- **Incident Responder / SOC Analyst**
  - Handles real-time incident detection, containment, and response.
  - Escalates and coordinates incident management efforts.

No two organizations are exactly the same.

Penetration Tester / Ethical Hacker

- Simulates attacks to identify weaknesses.
- Provides remediation guidance.

Threat Intelligence Analyst

- Tracks threat actors, TTPs, and emerging risks.
- Enriches defense posture with external intel.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Organizational Roles and Responsibilities

No two organizations are exactly the same.

Governance, Risk, and Compliance (GRC) Roles

- Risk Analyst / Risk Manager
  - Identifies, assesses, and mitigates information security risks.
  - Works closely with business units on risk decisions.
- Policy & Audit Analyst
  - Develops policies, standards, and procedures.
  - Conducts internal audits and supports external assessments
- Third-Party Risk Analyst
  - Evaluates and monitors security risks posed by vendors and partners.
  - Manages due diligence and assessments.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Organizational Roles and Responsibilities

No two organizations are exactly the same.

Specialized or Supporting Roles

- **Data Privacy Officer**
  - Oversees compliance with privacy laws (e.g., GDPR, CCPA).
  - Works with legal and security on personal data protection.
- **Security Software Developer / DevSecOps Engineer**
  - Integrates security into the software development lifecycle (SDLC).
  - Automates security testing and deployment.
- **Cloud Security Engineer**
  - Secures cloud platforms (AWS, Azure, GCP).
  - Manages identity, encryption, and configuration.

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Security Control Frameworks

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Security Control Frameworks

Structured set of guidelines, best practices, and controls designed to help organizations manage risk, protect information assets, and ensure compliance with legal, regulatory, or industry standards. It provides a repeatable and measurable approach to building, implementing, and maintaining an effective security program.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Security Control Frameworks

International Organization for Standardization (ISO)

A family of international standards for information security management, developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

- **ISO 27001**: The core standard—defines requirements for an Information Security Management System (ISMS).
- **ISO 27002**: Provides best practices and detailed guidance on security controls.
- **ISO 27000**: Gives foundational terms and concepts for the entire series.

The goal: help organizations systematically manage information security risks through governance, policies, and controls.

Use it if you need a globally recognized, risk-based framework to secure data and demonstrate trust.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Security Control Frameworks

National Institute of Standards and Technology (NIST)

A U.S. government agency that develops trusted security standards, guidelines, and best practices—widely used across public and private sectors to improve cybersecurity.

They're best known in infosec for frameworks like the **NIST Cybersecurity Framework (CSF)** and Special Publications such as **SP 800-53** (security controls) and **SP 800-171** (for protecting controlled unclassified information).

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Security Control Frameworks

Control Objectives for Information and Related Technologies (COBIT)

Framework for IT governance and management, developed by ISACA, that helps organizations align IT—including information security—with business goals, manage risk, and ensure compliance through structured processes and controls.

Based on **six key principles** for the governance and management of enterprise IT:

- Provide Stakeholder Value
- Holistic Approach
- Dynamic Governance System
- Governance Distinct from Management
- Tailored to Enterprise Needs
- End-to-End Governance System

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Security Control Frameworks

Sherwood Applied Business Security Architecture (SABSA)

A risk-driven security framework used to design and manage enterprise security architectures that align directly with business goals and requirements.

Unlike control-centric models, SABSA starts with business objectives and uses those to define security needs across layers—from strategy to policy to technology. It ensures that security is built in by design, not bolted on, and emphasizes traceability, accountability, and adaptability throughout the security lifecycle.

- Risk-focused
- Business-driven
- Layered approach
- Framework and methodology
- Certification

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Security Control Frameworks

Payment Card Industry Data Security Standard (PCI DSS)

A global security standard developed by the Payment Card Industry Security Standards Council (PCI SSC) to protect cardholder data and reduce credit card fraud.

Applies to all organizations that **store, process, or transmit payment card information** and outlines 12 core requirements focused on building secure networks, protecting data, managing vulnerabilities, implementing strong access controls, and monitoring systems.

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Security Control Frameworks

Federal Risk and Authorization Management Program (FedRAMP)

A widely adopted framework for IT service management (ITSM) that focuses on aligning IT services with business needs through standardized best practices.

ITIL emphasizes:

- Integrating security into all stages of IT service delivery
- Ensuring confidentiality, integrity, and availability (CIA) of data
- Defining and maintaining security policies, roles, and responsibilities
- Supporting risk management and compliance
- Promoting collaboration between IT security and other IT service functions

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Security Control Frameworks

Information Technology Infrastructure Library (ITIL)

- A a U.S. government-wide program that provides a **standardized approach** to security assessment, authorization, and continuous monitoring **for cloud services used by federal agencies**.
- Goal is to ensure that cloud service providers (CSPs) meet strict security and compliance requirements before they can be used by federal agencies.
- Uses a **"do once, use many" model**—meaning once a cloud service is authorized, multiple agencies can use it without repeating the full security assessment.
- Based on **NIST SP 800-53** controls and is required for any cloud provider doing business with the federal government.

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Due Diligence and Due Care

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Due Diligence and Due Care

Due Diligence = “Investigate before acting” = “Knowing what the risks are”

- It’s the research, analysis, and planning you do to understand risks and make informed decisions.
- Example: Before signing a contract with a cloud vendor, you review their security practices, certifications, and past breach history.

CHAPTER 1

Security Governance Through Principles and Policies

Manage the Security Function

Due Diligence and Due Care

Due Diligence = "Investigate before acting" = "Knowing what the risks are"

- It's the research, analysis, and planning you do to understand risks and make informed decisions.
- Example: Before signing a contract with a cloud vendor, you review their security practices, certifications, and past breach history.

Due Care = "Act responsibly based on what you know" = "Doing something responsible about them"

- It's the actual implementation of safeguards and actions to prevent harm, based on what you learned from due diligence.
- Example: After assessing the vendor, you enforce multi-factor authentication and require encryption for data in transit and at rest.

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Security Policy, Standards, Procedures, and Guidelines

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Security Policy, Standards, Procedures, and Guidelines

Security Policies

CHAPTER 1

Security Governance Through Principles and Policies

Security Policy, Standards, Procedures, and Guidelines

Security Policies

- **Formal, high-level documents** that define an organization's **rules, expectations, and responsibilities** for protecting information assets.
- Serve as the **foundation** of the security program, guiding decisions, behavior, and the implementation of controls.
- Common Characteristics:
  - Broad in scope and strategic in nature
  - Provide direction, not detailed instructions
  - Enforceable across the organization
  - Require regular review and updates
- Think of policies as the "**what and why**", with supporting standards and procedures handling the "**how**".

Compliance is mandatory.

CHAPTER 1

Security Governance Through Principles and Policies

Security Policy, Standards, Procedures, and Guidelines

Security Standards

- **Mandatory**, **detailed rules** that support the implementation of security policies.
- They ensure **consistency and uniformity** across technologies, processes, and environments.
- Examples:
  - All passwords must be at least 12 characters long and include special characters.
  - All laptops must have full-disk encryption using AES-256.
  - Firewalls must be configured to deny all inbound traffic by default.
- Standards turn policy directives into concrete, enforceable expectations.
- They often align with regulatory or industry frameworks.

Compliance is mandatory.

CHAPTER 1

Security Governance Through Principles and Policies

Security Policy, Standards, Procedures, and Guidelines

Security Baselines

- **Minimum acceptable security configurations** or settings for systems, applications, and devices.
- Ensure every system starts from a **known, secure configuration**, reducing variability and exposure.
- Examples:
  - A Windows 10 laptop baseline might include disabling SMBv1, enabling BitLocker, and enforcing secure boot.
  - A web server baseline might include TLS 1.2+, disabled directory browsing, and specific logging settings.
- Baselines are a subset of standards—they apply standards to specific platforms or technologies and define the least secure acceptable state.

Compliance is mandatory.

CHAPTER 1

Security Governance Through Principles and Policies

Security Policy, Standards, Procedures, and Guidelines

Security Guidelines

- **Recommended practices** that offer **flexibility** and **advice** on how to implement security in various contexts.
- Provide helpful, non-mandatory guidance when rigid standards don't fit every scenario.
- Examples:
  - Recommendations for securely using personal devices under a BYOD policy
  - Suggested password manager options for users
  - Guidance on writing secure code for developers
- Support policies and standards by giving **contextual best practices.**

Compliance is NOT mandatory.

CHAPTER 1

Security Governance Through Principles and Policies

Security Policy, Standards, Procedures, and Guidelines

Security Procedures

- **Detailed, step-by-step instructions** that describe exactly how to perform a specific task or process to meet the requirements of security policies, standards, and baselines.
- Ensure that security-related **activities are performed consistently, correctly, and securely**, regardless of who is performing them.
- Characteristics:
  - Highly detailed and specific
  - Usually technical or operational in nature
  - Created and maintained by practitioners (e.g., system admins, security analysts)
  - Often organized as playbooks, SOPs (Standard Operating Procedures), or runbooks

Compliance is mandatory.

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Threat Modeling

CHAPTER 1

Security Governance Through Principles and Policies

Threat Modeling

The structured process of **identifying, analyzing, and evaluating potential threats and vulnerabilities** to a system, application, or process **before** they can be exploited

proactive

CHAPTER 1

Security Governance Through Principles and Policies

Threat Modeling

The structured process of **identifying, analyzing, and evaluating potential threats and vulnerabilities** to a system, application, or process **before** they can be exploited

Purpose: To proactively understand **what could go wrong**, assess **who might attack**, and design **mitigations** to reduce risk—**before** building or deploying technology.

CHAPTER 1

Security Governance Through Principles and Policies

Threat Modeling

The structured process of **identifying, analyzing, and evaluating potential threats and vulnerabilities** to a system, application, or process **before** they can be exploited

Purpose: To proactively understand **what could go wrong**, assess **who might attack**, and design **mitigations** to reduce risk—**before** building or deploying technology.

How It Works (in simple terms):

1. **What are we building?** – Define the system, application, or environment.
2. **What can go wrong?** – Identify possible threats (e.g., spoofing, tampering, data leakage).
3. **What are we doing to protect it?** – Identify controls in place or needed.
4. **Is that enough?** – Evaluate risks and prioritize improvements.

CHAPTER 1

Security Governance Through Principles and Policies

Threat Modeling

The structured process of **identifying, analyzing, and evaluating potential threats and vulnerabilities** to a system, application, or process **before** they can be exploited

Purpose: To proactively understand **what could go wrong**, assess **who might attack**, and design **mitigations** to reduce risk—**before** building or deploying technology.

How It Works (in simple terms):

1. **What are we building?** – Define the system, application, or environment.
2. **What can go wrong?** – Identify possible threats (e.g., spoofing, tampering, data leakage).
3. **What are we doing to protect it?** – Identify controls in place or needed.
4. **Is that enough?** – Evaluate risks and prioritize improvements.

Common Methods: STRIDE, PASTA, DREAD, Attack Trees, Kill Chain/MITRE ATT&CK Mapping

CHAPTER 1

Security Governance Through Principles and Policies

Threat Modeling

The structured process of **identifying, analyzing, and evaluating potential threats and vulnerabilities** to a system, application, or process **before** they can be exploited

Purpose: To proactively understand **what could go wrong**, assess **who might attack**, and design **mitigations** to reduce risk—**before** building or deploying technology.

How It Works (in simple terms):

1. **What are we building?** – Define the system, application, or environment.
2. **What can go wrong?** – Identify possible threats (e.g., spoofing, tampering, data leakage).
3. **What are we doing to protect it?** – Identify controls in place or needed.
4. **Is that enough?** – Evaluate risks and prioritize improvements.

Common Methods: STRIDE, PASTA, DREAD, Attack Trees, Kill Chain/MITRE ATT&CK Mapping

Why It Matters:

- Helps build secure-by-design systems
- Prioritizes risk before incidents happen
- Informs architecture, security controls, and response planning

CHAPTER 1

Security Governance Through Principles and Policies

Threat Modeling

STRIDE (**S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, **E**levation of Privilege)

Six Types of Threats

Letter	Threat Type	What it Means (Simple)
S	Spoofing	Pretending to be someone else (e.g., logging in as another user).
T	Tampering	Changing data or code without permission (e.g., modifying a file or message).
R	Repudiation	Denying an action that was taken (e.g., “I didn’t send that request!”).
I	Information Disclosure	Exposing data to people who shouldn’t see it (e.g., data leaks).
D	Denial of Service	Disrupting or crashing a system so others can’t use it.
E	Elevation of Privilege	Gaining more access than you’re supposed to (e.g., a regular user becomes admin).

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Threat Modeling

STRIDE (**S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, **E**levation of Privilege)

Six Types of Threats

Letter	Threat Type	What it Means (Simple)
S	Spoofing	Pretending to be someone else (e.g., logging in as another user).
T	Tampering	Changing data or code without permission (e.g., modifying a file or message).
R	Repudiation	Denying an action that was taken (e.g., “I didn’t send that request!”).
I	Information Disclosure	Exposing data to people who shouldn’t see it (e.g., data leaks).
D	Denial of Service	Disrupting or crashing a system so others can’t use it
E	Elevation of Pr	

How You Use It

When you’re designing or reviewing a system:

1. Look at each component (e.g., login forms, APIs, databases).
2. Ask: “Could this be spoofed? Tampered with?…” for each STRIDE category.
3. Identify threats and put in controls (like encryption, logging, access restrictions) to reduce risk.

CHAPTER 1

Security Governance Through Principles and Policies

Threat Modeling

PASTA (Process for Attack Simulation and Threat Analysis)

Think of it as a **7-step recipe** for cooking up a deep understanding of threats—based on how a system actually works and what an attacker might realistically do.

Stage	What it Means (Simple)
I: Define the Objectives (DO)	Understand what the business cares about (e.g., protect customer data).
II: Definition of Technical Scope (DTS)	Document the system: architecture, users, components, data flows.
III: Application Decomposition and Analysis (ADA)	Break down the system into smaller parts to see where weaknesses might exist.
IV: Threat Analysis (TA)	Identify potential threats based on attacker goals and capabilities.
V: Weakness and Vulnerability Analysis (WVA)	Find technical weaknesses in the system.
VI: Attack Modeling & Simulation (AMS)	Simulate how attacks could happen using attack trees or kill chains.
VII: Risk Analysis & Management (RAM)	Recommend and prioritize defenses based on risk and impact.

CHAPTER 1

Security Governance Through Principles and Policies

Threat Modeling

DREAD (**D**amage, **R**eproducibility, **E**xploitability, **A**ffected Users, and **D**iscoverability)

A simple way to rate and prioritize security threats based on how dangerous they are. It's often used after identifying threats (like through STRIDE or PASTA) to figure out which ones to fix first.

Letter	Factor	What it Means (Simple)
D	Damage Potential	How bad would it be if the threat happened? (e.g., data loss, downtime)
R	Reproducibility	How easy is it to repeat the attack over and over?
E	Exploitability	How easy is it for an attacker to launch the attack? (Tools, access, skill)
A	Affected Users	How many people or systems would be impacted?
D	Discoverability	How easy is it to find the weakness or vulnerability?

How to Use It:

- Give each factor a score (e.g., 1–10)
- Add them up to get a risk score for each threat
- Higher total = bigger risk = higher priority

2025 CISSP MENTOR PROGRAM

CHAPTER 1

Security Governance Through Principles and Policies

Supply Chain Risk Management

Protecting the organization from information security risks that come through third parties—like vendors, partners, contractors, software providers, and service providers.

CHAPTER 1

Security Governance Through Principles and Policies

Supply Chain Risk Management (SCRM)

Protecting the organization from information security risks that come through third parties—like vendors, partners, contractors, software providers, and service providers.

- **SLR (Service Level Requirement)** - A documented customer expectation for a specific level of service performance (e.g., 99.9% uptime).
- **SLA (Service Level Agreement)** - A formal agreement between a provider and a customer that defines the agreed-upon level of service, including metrics, responsibilities, and penalties.

CHAPTER 1

Security Governance Through Principles and Policies

Supply Chain Risk Management (SCRM)

Protecting the organization from information security risks that come through third parties—like vendors, partners, contractors, software providers, and service providers.

- **SLR (Service Level Requirement)** - A documented customer expectation for a specific level of service performance (e.g., 99.9% uptime).
- **SLA (Service Level Agreement)** - A formal agreement between a provider and a customer that defines the agreed-upon level of service, including metrics, responsibilities, and penalties.
- **Silicon Root of Trust (RoT)** - A security feature built directly into a computer chip that acts as a trusted starting point for verifying that a system's hardware and software haven't been tampered with when it boots up.
- **Physically Unclonable Function (PUF)** - A unique and unpredictable fingerprint created by tiny imperfections in a computer chip's hardware during manufacturing, used to securely identify and authenticate devices. ("digital snowflake")
- **Software Bill of Materials (SBOM)** - A list of all the components and dependencies that make up a piece of software, like an ingredient label for code.

CHAPTER 1

Security Governance Through Principles and Policies

You survived CHAPTER 1, CONGRATS!

Review the ”Summary” and “Study Essentials” in the book.

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

CHAPTER 2

Personnel Security and Risk Management Concepts

Things to cover in this chapter:

- Personnel Security Policies and Procedures
- Understand and Apply Risk Management Concepts
- Social Engineering
- Establish and Maintain a Security Awareness, Education, and Training Program

The chapter starts off with "*Humans are often considered the weakest element in any security solution.*"

What do you think, are humans the "weakest element"?

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Things to cover in this chapter:

> *“Technology is simple to secure—computers only do what you tell them to do. People are the real challenge—they do what they want to do.”*
>
> – Me ☺

What do you think, are humans the “weakest element”?

CHAPTER 2

Personnel Security and Risk Management Concepts

Job Descriptions and Responsibilities

In information security, clear job descriptions and defined responsibilities are critical because they:

1. **Establish Accountability** - When everyone knows their security-related duties, there's no ambiguity about **who is responsible** for protecting data, reporting incidents, or following procedures. Accountability reduces the risk of negligence.
2. **Support Least Privilege and Access Control** - Well-defined roles help ensure people only have access to the systems and data they need for their job—nothing more. This is foundational for implementing least privilege and minimizing insider threats.
3. **Align with Policies, Training & Audits** - Security policies and training are most effective when tailored to specific roles. Auditors also look for alignment between roles, responsibilities, and system access, making job descriptions key for compliance.

CHAPTER 2

Personnel Security and Risk Management Concepts

Job Descriptions and Responsibilities

In information security, clear job descriptions and defined responsibilities are critical because they:

4. **Reduce Human Error and Security Gaps** - Security lapses often happen when people don't know what they're supposed to do—or think "someone else is handling it." Clear responsibilities reduce assumptions and confusion.
5. **Enable Incident Response & Continuity** - During a security incident, it's essential to know who does what—from detection to communication to recovery. Job descriptions help coordinate an effective response and keep operations running.

Bottom line:

Without clear job descriptions and responsibilities, your people become the weakest link. With them, they become one of your strongest security controls.

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Candidate Screening and Hiring

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Candidate Screening and (secure) Hiring (practices)

CHAPTER 2

Personnel Security and Risk Management Concepts

Candidate Screening and (secure) Hiring (practices)

Essential because they help ensure that the people you bring into the organization are **trustworthy**, **qualified**, and don’t pose an unaccounted for (or unnecessary) risk.

CHAPTER 2

Personnel Security and Risk Management Concepts

Candidate Screening and (secure) Hiring (practices)

Essential because they help ensure that the people you bring into the organization are **trustworthy**, **qualified**, and don't pose an unaccounted for (or unnecessary) risk.

1. Reduce Insider Threat Risk - Not all threats come from the outside. Malicious insiders, or even well-intentioned but careless employees, can cause serious damage. Background checks and screening help identify red flags before someone gets access to sensitive data.

CHAPTER 2

Personnel Security and Risk Management Concepts

Candidate Screening and (secure) Hiring (practices)

Essential because they help ensure that the people you bring into the organization are **trustworthy**, **qualified**, and don't pose an unaccounted for (or unnecessary) risk.

1. **Reduce Insider Threat Risk** - Not all threats come from the outside. Malicious insiders, or even well-intentioned but careless employees, can cause serious damage. Background checks and screening help identify red flags before someone gets access to sensitive data.
2. **Verify Skills and Trustworthiness** - Security isn't just about tech—it's about people making the right decisions. Screening ensures candidates have the right experience, ethical judgment, and mindset to follow security policies and handle sensitive responsibilities.

CHAPTER 2

Personnel Security and Risk Management Concepts

Candidate Screening and (secure) Hiring (practices)

Essential because they help ensure that the people you bring into the organization are **trustworthy**, **qualified**, and don't pose an unaccounted for (or unnecessary) risk.

1. **Reduce Insider Threat Risk** - Not all threats come from the outside. Malicious insiders, or even well-intentioned but careless employees, can cause serious damage. Background checks and screening help identify red flags before someone gets access to sensitive data.
2. **Verify Skills and Trustworthiness** - Security isn't just about tech—it's about people making the right decisions. Screening ensures candidates have the right experience, ethical judgment, and mindset to follow security policies and handle sensitive responsibilities.
3. **Support Regulatory Compliance** - Many standards (like ISO 27001, PCI-DSS, or NIST) require organizations to screen personnel prior to hire—especially those in sensitive or privileged roles.

CHAPTER 2

Personnel Security and Risk Management Concepts

Candidate Screening and (secure) Hiring (practices)

Essential because they help ensure that the people you bring into the organization are **trustworthy**, **qualified**, and don’t pose an unaccounted for (or unnecessary) risk.

4. **Protect Access from Day One** - Hiring the wrong person can put your systems at risk the moment they’re onboarded. Proper screening helps ensure only trusted individuals gain access to your network, systems, and data.

CHAPTER 2

Personnel Security and Risk Management Concepts

Candidate Screening and (secure) Hiring (practices)

Essential because they help ensure that the people you bring into the organization are **trustworthy**, **qualified**, and don't pose an unaccounted for (or unnecessary) risk.

4. **Protect Access from Day One** - Hiring the wrong person can put your systems at risk the moment they're onboarded. Proper screening helps ensure only trusted individuals gain access to your network, systems, and data.
5. **Build a Culture of Security and Responsibility** - When candidates know security is taken seriously—even during hiring—it sets a tone that security is everyone's responsibility, starting from the moment someone applies.

Bottom line:

You can have the best firewalls in the world—but if you hire the wrong people, they can walk right through them.

CHAPTER 2

Personnel Security and Risk Management Concepts

Candidate Screening and (secure) Hi

1. Define Role-Based Security Requirements

- Identify which roles have access to sensitive systems, data, or privileged functions.
- Establish screening levels based on the sensitivity of the role (e.g., IT admins vs. general staff).

2. Conduct Background Checks (Pre-Employment Screening)

- Verify identity, employment history, and education.
- Perform criminal background checks, where legally permitted.
- Check credit history for roles involving financial responsibility.
- Validate professional certifications (e.g., CISSP, CEH) and references.

For high-trust roles (e.g., vCISOs, sysadmins, developers), use more rigorous checks.

3. Assess Cultural and Ethical Fit

- Evaluate the candidate's attitude toward rules, compliance, and responsibility.
- Use situational or behavioral interview questions to probe judgment and integrity.
- For some roles, psychometric or integrity testing may be appropriate.

4. Enforce Clear Contracts and Agreements

- Require signed NDAs (Non-Disclosure Agreements).
- Include clauses for acceptable use, confidentiality, and security policy adherence.
- For high-risk roles, include language about intellectual property, access revocation, and termination procedures.

5. Provide Security Orientation and Training at Onboarding

- Don't wait. Train new hires on security policies, acceptable use, phishing awareness, and incident reporting right away.
- Make sure they understand that security is part of their job, not someone else's problem.

6. Maintain a Process for Continuous Monitoring (Where Appropriate)

- For certain critical roles, periodically re-screen employees (e.g., every 2–3 years).
- Watch for behavioral changes, policy violations, or access anomalies as part of insider threat detection.

7. Have a Secure Offboarding Process

- Immediately revoke access upon resignation or termination.
- Recover company-owned devices, tokens, and badges.
- Remind the departing employee of their continuing obligations (e.g., confidentiality)

BONUS: Document Everything

- Keep records of screenings, signed agreements, and onboarding steps.
- This supports compliance with standards (ISO, NIST, etc.) and helps in case of an investigation.

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Onboarding: Employment Agreements and Policy-Driven Requirements

A critical step that sets the tone for a security-aware workforce from day one. It's where legal, procedural, and cultural expectations around protecting information assets are clearly established and agreed upon.

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Onboarding: Employment Agreements and Policy-Driven Requirements

A critical step that sets the tone for a security-aware workforce from day one. It’s where legal, procedural, and cultural expectations around protecting information assets are clearly established and agreed upon.

1. **Establishes Legal and Ethical Accountability**
   - Employment agreements often include confidentiality clauses, NDAs, IP protections, and acceptable use terms.
   - Signing these documents makes it clear that the employee is legally bound to protect sensitive information and follow security protocols.

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Onboarding: Employment Agreements and Policy-Driven Requirements

A critical step that sets the tone for a security-aware workforce from day one. It's where legal, procedural, and cultural expectations around protecting information assets are clearly established and agreed upon.

1. **Establishes Legal and Ethical Accountability**
   - Employment agreements often include confidentiality clauses, NDAs, IP protections, and acceptable use terms.
   - Signing these documents makes it clear that the employee is legally bound to protect sensitive information and follow security protocols.
2. **Reinforces Security as a Job Requirement**
   - By acknowledging policies (e.g., acceptable use, data handling, password management), employees are shown that security isn't optional—it's part of the job.
   - It eliminates the excuse of "I didn't know."

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Onboarding: Employment Agreements and Policy-Driven Requirements

A critical step that sets the tone for a security-aware workforce from day one. It’s where legal, procedural, and cultural expectations around protecting information assets are clearly established and agreed upon.

3. Reduces Risk of Insider Threats
    - Clear expectations reduce the chances of **negligent or malicious behavior**.
    - In case of a policy violation or incident, the agreements provide **legal and disciplinary recourse**.

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Onboarding: Employment Agreements and Policy-Driven Requirements

A critical step that sets the tone for a security-aware workforce from day one. It’s where legal, procedural, and cultural expectations around protecting information assets are clearly established and agreed upon.

3. **Reduces Risk of Insider Threats**
   - Clear expectations reduce the chances of **negligent or malicious behavior**.
   - In case of a policy violation or incident, the agreements provide **legal and disciplinary recourse**.
4. **Provides a Foundation for Training and Culture**
   - Onboarding is the best time to explain the “why” behind the rules, building understanding and buy-in for the security culture.
   - A well-structured onboarding program gives employees the tools they need to make secure decisions right away.

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Onboarding: Employment Agreements and Policy-Driven Requirements

A critical step that sets the tone for a security-aware workforce from day one. It's where legal, procedural, and cultural expectations around protecting information assets are clearly established and agreed upon.

5. **Ensures Compliance and Audit Readiness**
   - Standards like ISO 27001, NIST, and PCI-DSS require documented evidence that employees are aware of and accept their security responsibilities.
   - Proper onboarding helps you prove compliance and pass audits.

What It Should Include:

- Signed employment agreement with security clauses
- Acknowledgment of security policies (e.g., acceptable use, remote access)
- Security awareness orientation or training
- Role-specific requirements (e.g., MFA use, encryption tools)
- Explanation of incident reporting procedures

Bottom line:

- Onboarding is where security begins.
- It's your chance to turn new hires into security allies—with clear rules, shared responsibility, and the right mindset from the start.

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Onboarding: Employment Agreements and Policy-Driven Requirements

Important Terms:

- **Onboarding** - process of integrating new personnel into an organization by providing them with access, training, and documentation—while ensuring they understand and agree to security policies and responsibilities.
- **Identity and access management (IAM)** - the framework of policies and technologies used to ensure the right individuals have the appropriate access to resources at the right times and for the right reasons.
- **Principle of least privilege** - the security concept of granting users and systems the minimum level of access necessary to perform their duties—no more, no less.
- **Nondisclosure agreement (NDA)** - a legal contract that requires individuals to protect confidential information from unauthorized disclosure or use.
- **Mandatory vacations** - a security control that requires employees to take time off, helping to detect fraud or malicious activity that might be hidden through continuous control of their duties.

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Onboarding: Employment Agreements and Policy-Driven Requirements

Important Terms:

- **Collusion** - a security risk where two or more individuals conspire to commit fraud or bypass security controls.
- **User Behavior Analytics (UBA)** - use of data analytics to monitor and analyze user activity to detect abnormal or risky behavior that may indicate a security threat.
- **User and Entity Behavior Analytics (UEBA)** - expands on UBA by also analyzing non-human entities (like devices, applications, or servers) to detect suspicious or anomalous behavior across the environment.
- **Offboarding** - formal process of revoking access, recovering assets, and reinforcing security obligations when an employee or contractor leaves an organization.

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Offboarding, Transfers, and Termination Processes

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Offboarding, Transfers, and Termination Processes

Secure Offboarding Steps (Voluntary & Involuntary)

1. **Plan the Offboarding (If Possible)**
   - Voluntary: Coordinate ahead of the departure date (2-week notice, etc.).
   - Involuntary: Prepare discreetly before termination to prevent sabotage or data theft.

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Offboarding, Transfers, and Termination Processes

Secure Offboarding Steps (Voluntary & Involuntary)

1. **Plan the Offboarding (If Possible)**
   - Voluntary: Coordinate ahead of the departure date (2-week notice, etc.).
   - Involuntary: Prepare discreetly before termination to prevent sabotage or data theft.
2. **Revoke Access Immediately After Departure (or During Notification)**
   - Disable all accounts: email, VPN, cloud platforms, remote desktop, etc.
   - Remove from access groups, shared drives, MFA systems, and internal tools.
   - For involuntary terminations, do this simultaneously with the separation conversation.

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Offboarding, Transfers, and Termination Processes

Secure Offboarding Steps (Voluntary & Involuntary)

1. **Plan the Offboarding (If Possible)**
   - Voluntary: Coordinate ahead of the departure date (2-week notice, etc.).
   - Involuntary: Prepare discreetly before termination to prevent sabotage or data theft.
2. **Revoke Access Immediately After Departure (or During Notification)**
   - Disable all accounts: email, VPN, cloud platforms, remote desktop, etc.
   - Remove from access groups, shared drives, MFA systems, and internal tools.
   - For involuntary terminations, do this simultaneously with the separation conversation.
3. **Recover All Company Assets**
   - Collect laptops, phones, ID badges, tokens, keys, USBs, and documentation.
   - Log serial numbers and condition of returned equipment.
   - Use a checklist to avoid missed items.

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Offboarding, Transfers, and Termination Processes

Secure Offboarding Steps (Voluntary & Involuntary)

4. **Preserve and Secure Business Data**
    - Back up the employee’s:
        - Email inbox
        - Files and folders
        - Chat messages (if business-related)
        - Logs of system activity (for review if needed)

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Offboarding, Transfers, and Termination Processes

Secure Offboarding Steps (Voluntary & Involuntary)

4. **Preserve and Secure Business Data**
   - Back up the employee's:
     - Email inbox
     - Files and folders
     - Chat messages (if business-related)
     - Logs of system activity (for review if needed)
5. **Reinforce Legal and Security Obligations**
   - Remind them of signed **NDAs**, intellectual property clauses, and post-employment restrictions.
   - In **involuntary cases**, issue written notice confirming their ongoing obligations.

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Offboarding, Transfers, and Termination Processes

Secure Offboarding Steps (Voluntary & Involuntary)

6. **Notify Internal Teams**
   - Inform IT, security, HR, and management of the separation.
   - Remove them from contact lists, org charts, and communication channels.
   - Reassign open tasks or access-dependent responsibilities.

CHAPTER 2

Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

Offboarding, Transfers, and Termination Processes

Secure Offboarding Steps (Voluntary & Involuntary)

6. **Notify Internal Teams**
   - Inform IT, security, HR, and management of the separation.
   - Remove them from contact lists, org charts, and communication channels.
   - Reassign open tasks or access-dependent responsibilities.
7. **Conduct an Exit Interview (Voluntary only)**
   - Ask for feedback.
   - Clarify that systems remain monitored post-departure.
   - Thank them professionally—security and respect go hand in hand.

Bonus: Monitor for Post-Departure Risks

Watch for:

- Unusual logins (from devices or accounts that weren't deactivated)
- Data exfiltration before departure
- Contact with former teammates using unofficial channels

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Information security IS risk management!

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

In order to manage risk, we should know what risk is first.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

In order to manage risk, we should know what risk is first.

Risk = Likelihood × Impact

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

In order to manage risk, we should know what risk is first.

Risk = Likelihood × Impact

In simple terms:

Risk is the likelihood that something bad will happen, and how bad it would be if it did.

In information security, this means thinking about:

- **How likely** it is that a threat (like a hacker, accident, or failure) will exploit a vulnerability
- **How much damage** it would cause to systems, data, operations, or reputation

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

In order to manage risk, we should know what risk is first.

Risk = Likelihood × Impact

In simple terms:

Risk is the likelihood that something bad will happen, and how bad it would be if it did.

In information security, this means thinking about:

- **How likely** it is that a threat (like a hacker, accident, or failure) will exploit a vulnerability
- **How much damage** it would cause to systems, data, operations, or reputation

Managing risk is all about reducing risk (the likelihood, the impact, or both) and maintaining it at an acceptable level.

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Definitions in context:

- **Threat** = Something capable of causing harm (e.g., attacker, natural disaster)
- **Vulnerability** = A weakness that could be exploited (e.g., outdated software)
- **Impact** = The damage or consequence if the exploit succeeds (e.g., breached data)

Risk is the likelihood that something bad will happen, and how bad it would be if it did.

This is a threat exploiting a vulnerability

In information security, this means thinking about:

- **How likely** it is that a threat (like a hacker, acci nerability
- **How much damage** it would cause to systems,

Managing risk is all about reducing risk (the likelihood, the impact, or both) and maintaining it at an <u>acceptable</u> level.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Now that I know what "risk" is, next is to figure out what our risks are.

This requires a risk assessment (aka risk analysis).

Lots of things come into play (focused on determining likelihoods and impacts):

- **Asset** - anything of value to the organization that needs protection—such as data, systems, hardware, software, or even people.
- **Asset Valuation** - process of determining the worth or importance of an asset to the organization, to help prioritize protection based on potential impact if compromised.
- **Threats** - any potential causes of harm that can exploit a vulnerability to negatively impact an asset.
- **Threat agents (or actors)** - individuals, groups, or entities that carry out or attempt to carry out threats against information assets.
- **Threat events** - specific occurrences where a threat agent attempts to exploit a vulnerability, potentially leading to harm or loss.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Now that I know what “risk” is, next is to figure out what our risks are.

This requires a risk assessment (aka risk analysis).

Lots of things come into play (focused on determining likelihoods and impacts):

- **Threat vector** - the path or method a threat agent uses to exploit a vulnerability and carry out an attack.
- **Vulnerability** - a weakness or flaw in a system, process, or control that can be exploited by a threat to cause harm.
- **Exposure** - the state of being vulnerable to a threat due to a lack of sufficient safeguards or controls.
- **Safeguards** - the security controls or countermeasures put in place to reduce risk by preventing, detecting, or responding to threats.
- An **attack** - a deliberate attempt by a threat agent to exploit a vulnerability and compromise the confidentiality, integrity, or availability of an asset.
- **Breach** - when a security mechanism is bypassed or successfully exploited by a threat agent (a successful attack).

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Now that I know what “risk” is, next is to figure out what our risks are.

This requires a risk assessment (aka risk analysis).

There are lots of ways to do risk assessments.

There are lots of ways to calculate the value of an asset (asset valuation).

There are lots of ways to identify threats (perspective really matters here).

There are lots of ways to identify vulnerabilities (perspective really matters here too).

Risk is ALWAYS relative. It’s never zero and it’s never infinite. It’s always somewhere in between. The only exceptions are where there are no threats and/or no vulnerabilities.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Qualitative Risk Analysis

The process of evaluating risks using descriptive ratings—like ***high***, ***medium***, *or* ***low***—based on expert judgment, experience, and available data, without relying on exact numbers.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Qualitative Risk Analysis

The process of evaluating risks using descriptive ratings—like ***high***, ***medium***, *or* ***low***—based on expert judgment, experience, and available data, without relying on exact numbers.

- It's like using a heat map or gut-check with structure to quickly figure out which risks matter most.
- **How it Works:**
  - Identify threats and vulnerabilities
  - Estimate likelihood and impact using categories (e.g., "Likely" or "Severe")
  - Use a **risk matrix** to prioritize which risks to address first

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Qualitative Risk Analysis

The process of evaluating risks using descriptive ratings—like ***high***, ***medium***, *or* ***low***—based on expert judgment, experience, and available data, without relying on exact numbers.

- It’s like using a heat map or gut-check with structure to quickly figure out which risks matter most.
- **How it Works:**
  - Identify threats and vulnerabilities
  - Estimate likelihood and impact using categories (e.g., “Likely” or “Severe”)
  - Use a **risk matrix** to prioritize which risks to address first
- **Why It’s Useful:**
  - Quick and easy to perform
  - Great when hard data is missing
  - Helps guide decisions and resource allocation

CHAPTER 2

Personnel Security and Risk Management C

Understand and Apply Risk Management Concepts

Quantitative Risk Analysis

The process of assigning numerical values (like dollars and probabilities) to estimate the financial impact of risks—so you can make more data-driven decisions.

Common Misconception:
Dollars is NOT the only method of quantification.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Quantitative Risk Analysis

The process of assigning numerical values (like dollars and probabilities) to estimate the financial impact of risks—so you can make more data-driven decisions.

- It’s like doing **security math** to figure out how much a risk could actually cost you.
- **How it Works:**
    - Estimate the asset value (AV)
    - Determine exposure factor (EF) – % of loss if an incident happens
    - Calculate Single Loss Expectancy (SLE) → AV × EF
    - Estimate how often it might happen per year → Annual Rate of Occurrence (ARO)
    - Calculate Annual Loss Expectancy (ALE) → SLE × ARO

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Quantitative Risk Analysis

The process of assigning numerical values (like dollars and probabilities) to estimate the financial impact of risks—so you can make more data-driven decisions.

- It's like doing **security math** to figure out how much a risk could actually cost you.
- **How it Works:**
  - Estimate the asset value (AV)
  - Determine exposure factor (EF) – % of loss if an incident happens
  - Calculate Single Loss Expectancy (SLE) → AV × EF
  - Estimate how often it might happen per year → Annual Rate of Occurrence (ARO)
  - Calculate Annual Loss Expectancy (ALE) → SLE × ARO
- **Why It's Useful:**
  - Helps justify security budgets and cost-benefit decisions
  - Supports ROI calculations for controls
  - Useful for insurance and compliance reporting

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and R

Understand and Apply Risk Management Concepts

Quantitative Risk Analysis

ate the

Quantitative Risk Analysis Example

Scenario:
You manage a file server that contains sensitive customer data. You want to calculate the Annual Loss Expectancy (ALE) if the server gets hit by ransomware.

Step-by-Step Calculation

1. **Asset Value (AV)**: The data and system are worth $100,000 to your organization.
2. **Exposure Factor (EF)**: If ransomware hits, you estimate 40% of the asset value would be lost (due to downtime, recovery costs, lost revenue, etc.). So, EF = 0.40
3. **Single Loss Expectancy (SLE)**: SLE = AV × EF = $100,000 × 0.40 = $40,000
4. **Annual Rate of Occurrence (ARO)**: Based on past incidents and threat intel, you estimate this could happen once every 2 years. So, ARO = 0.5
5. **Annual Loss Expectancy (ALE)**: ALE = SLE × ARO = $40,000 × 0.5 = $20,000

Interpretation

You can expect to lose $20,000 per year (on average) due to ransomware risk on that file server.

Now What?

You use this info to:

- Justify a $10,000/year backup and response solution, which saves money over time.
- Show leadership the value of investing in proactive risk reduction.

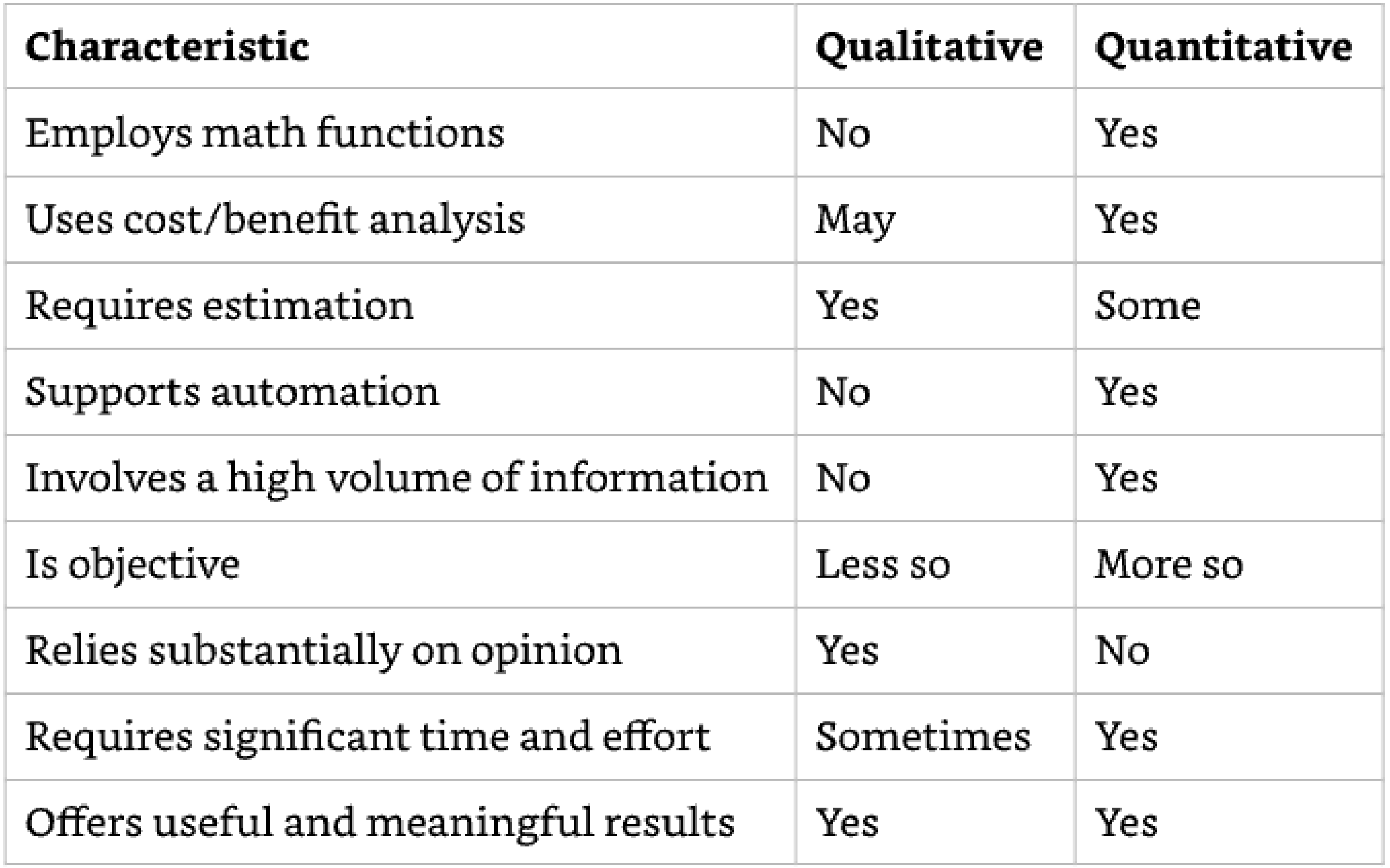
2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Manage

Risk assessment/analysis is NOT risk management, it's a step in risk management. Now, we need to make risk decisions!

Understand and Apply Risk Management Concepts



Characteristic	Qualitative	Quantitative
Employs math functions	No	Yes
Uses cost/benefit analysis	May	Yes
Requires estimation	Yes	Some
Supports automation	No	Yes
Involves a high volume of information	No	Yes
Is objective	Less so	More so
Relies substantially on opinion	Yes	No
Requires significant time and effort	Sometimes	Yes
Offers useful and meaningful results	Yes	Yes

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Risk Responses

You have six valid choices (risk ignorance is **NOT** a valid choice):

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Risk Responses

You have six valid choices (risk ignorance is **NOT** a valid choice):

1. **Risk Mitigation** - Reducing the risk by implementing controls or safeguards to lower its likelihood or impact.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Risk Responses

You have six valid choices (risk ignorance is **NOT** a valid choice):

1. **Risk Mitigation** - Reducing the risk by implementing controls or safeguards to lower its likelihood or impact.
2. **Risk Assignment** (or Transference) - Shifting the risk to a third party, such as through insurance or outsourcing.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Risk Responses

You have six valid choices (risk ignorance is **NOT** a valid choice):

1. **Risk Mitigation** - Reducing the risk by implementing controls or safeguards to lower its likelihood or impact.
2. **Risk Assignment** (or Transference) - Shifting the risk to a third party, such as through insurance or outsourcing.
3. **Risk Deterrence** - Discouraging threat actors by implementing measures like policies, penalties, or warnings.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Risk Responses

You have six valid choices (risk ignorance is **NOT** a valid choice):

1. **Risk Mitigation** - Reducing the risk by implementing controls or safeguards to lower its likelihood or impact.
2. **Risk Assignment** (or Transference) - Shifting the risk to a third party, such as through insurance or outsourcing.
3. **Risk Deterrence** - Discouraging threat actors by implementing measures like policies, penalties, or warnings.
4. **Risk Avoidance** - Eliminating the risk entirely by choosing not to engage in the risky activity.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Risk Responses

You have six valid choices (risk ignorance is **NOT** a valid choice):

1. **Risk Mitigation** - Reducing the risk by implementing controls or safeguards to lower its likelihood or impact.
2. **Risk Assignment** (or Transference) - Shifting the risk to a third party, such as through insurance or outsourcing.
3. **Risk Deterrence** - Discouraging threat actors by implementing measures like policies, penalties, or warnings.
4. **Risk Avoidance** - Eliminating the risk entirely by choosing not to engage in the risky activity.
5. **Risk Acceptance** - Acknowledging and tolerating the risk without taking action, usually because it's low or cost-prohibitive to address.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Risk Responses

You have six valid choices (risk ignorance is **NOT** a valid choice):

1. **Risk Mitigation** - Reducing the risk by implementing controls or safeguards to lower its likelihood or impact.
2. **Risk Assignment** (or Transference) - Shifting the risk to a third party, such as through insurance or outsourcing.
3. **Risk Deterrence** - Discouraging threat actors by implementing measures like policies, penalties, or warnings.
4. **Risk Avoidance** - Eliminating the risk entirely by choosing not to engage in the risky activity.
5. **Risk Acceptance** - Acknowledging and tolerating the risk without taking action, usually because it's low or cost-prohibitive to address.
6. **Risk Rejection** - Ignoring or denying the existence of a risk, which is not a recommended or responsible response.

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Cybersecurity Insurance

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Cybersecurity Insurance

(also called cyber liability insurance) is designed to protect organizations financially from the fallout of cyber incidents—such as data breaches, ransomware attacks, business interruption, and legal costs.

Pros of Cybersecurity Insurance

1. **Financial Protection** - Covers losses related to data breaches, business downtime, legal fees, fines, and incident response.
2. **Access to Expert Help** - Insurers often provide breach response teams, including forensic investigators, legal counsel, and PR specialists.
3. **Risk Transfer** - Reduces the organization's direct financial burden by shifting some risk to the insurer.
4. **Regulatory Support** - Helps manage compliance penalties or regulatory investigations (e.g., GDPR, HIPAA).
5. **Encourages Security Maturity** - The underwriting process often forces companies to improve their cybersecurity posture to qualify for coverage.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Cybersecurity Insurance

(also called cyber liability insurance) is designed to protect organizations financially from the fallout of cyber incidents—such as data breaches, ransomware attacks, business interruption, and legal costs.

Cons of Cybersecurity Insurance

1. **Not a Substitute for Good Security** - Insurance doesn't stop breaches—it just helps pay for the consequences. Weak controls can still lead to major damage.
2. **Coverage Gaps & Fine Print** - Policies may exclude certain types of attacks, such as nation-state threats or insider incidents, unless explicitly covered.
3. **Claims Can Be Denied** - If the organization fails to meet security obligations (e.g., didn't patch systems), insurers may reject the claim.
4. **Can Create Complacency** - Over-reliance on insurance might lead some organizations to underinvest in actual security controls.
5. **Rising Premiums** - Due to the increasing frequency and severity of cyberattacks, costs are going up, and coverage is getting harder to obtain.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Cybersecurity Insurance

(also called cyber liability insurance) is designed to protect organizations financially from the fallout of cyber incidents—such as data breaches, ransomware attacks, business interruption, and legal costs.

Cons of Cybersecurity Insurance

1. **Not a Substitute for Good Security** - Insurance doesn't stop breaches—it just helps pay for the consequences. Weak controls can still lead to major damage.
2. **Coverage Gaps & Fine Print** - Policies may exclude certain types of attacks, such as nation-state threats or insider incidents, unless explicitly covered.
3. **Claims Can Be Denied** - If the organization fails to meet security obligations (e.g., didn't patch systems), insurers may reject the claim.
4. **Can Create Complacency** - Over-reliance on insurance might lead some organizations to underinvest in actual security controls.
5. **Rising Premiums** - Due to the increasing frequency and severity of cyberattacks, costs are going up,

Bottom Line:

- Cyber insurance is a valuable safety net, but it should complement—not replace—a strong security program.
- Think of it as your financial firewall, not your first line of defense.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

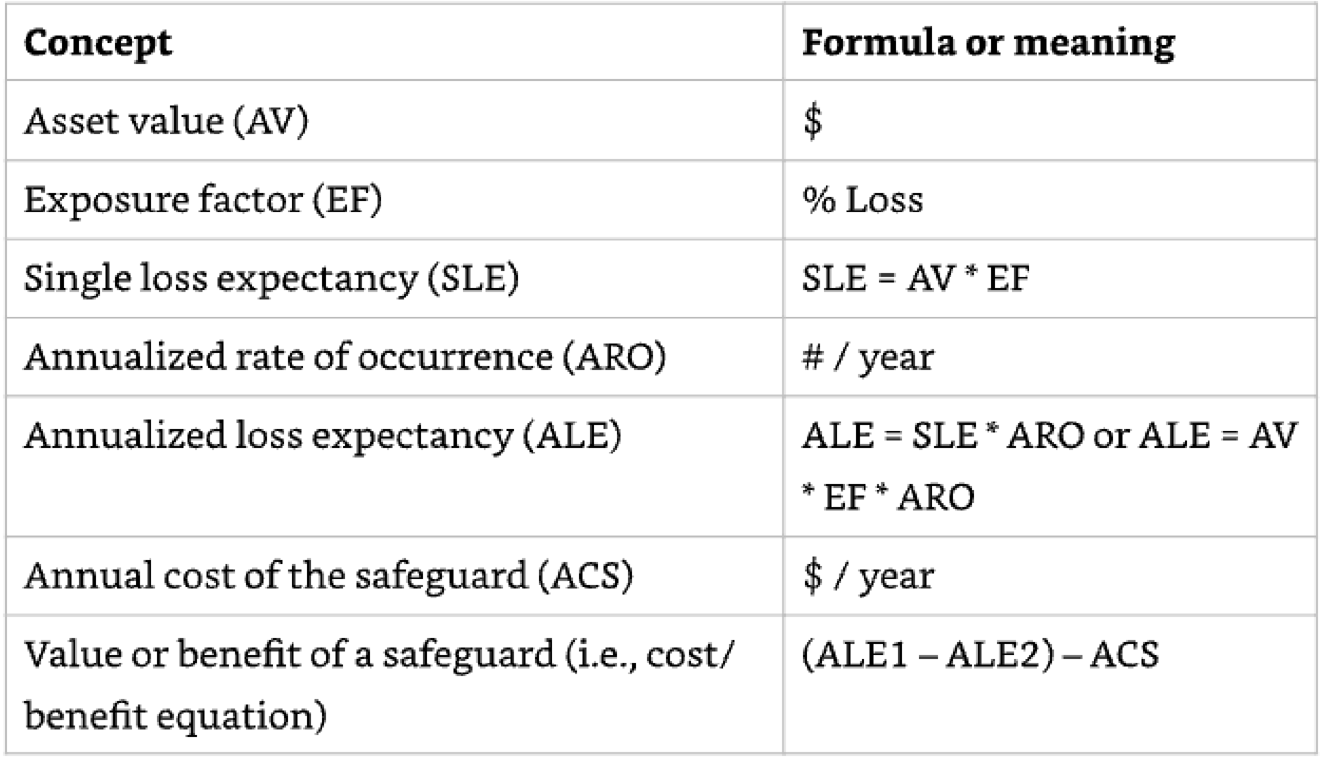
Countermeasure Selection and Implementation

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation



Concept	Formula or meaning
Asset value (AV)	$
Exposure factor (EF)	% Loss
Single loss expectancy (SLE)	SLE = AV * EF
Annualized rate of occurrence (ARO)	# / year
Annualized loss expectancy (ALE)	ALE = SLE * ARO or ALE = AV * EF * ARO
Annual cost of the safeguard (ACS)	$ / year
Value or benefit of a safeguard (i.e., cost/benefit equation)	(ALE1 – ALE2) – ACS

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Categories)

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Categories)

Administrative Controls

Also called managerial controls, these are policies, procedures, and guidelines that shape behavior and enforce security.

Examples:

- Security policies and standards
- Background checks and hiring practices
- Security training and awareness programs
- Incident response plans
- Access reviews and audits

Purpose: To influence and enforce human behavior and support governance.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Categories)

Technical (or Logical) Controls

These are technology-based controls used to enforce security policies and protect systems and data.

Examples:

- Firewalls and intrusion detection systems (IDS/IPS)
- Encryption and multi-factor authentication (MFA)
- Access control lists (ACLs)
- Antivirus and endpoint protection
- Data loss prevention (DLP) systems

Purpose: To protect systems and data directly through technology.

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Categories)

Technical (or Logical) Controls

These are controls that prevent physical access to IT systems, facilities, or data by unauthorized individuals.

Examples:

- Locks and fences
- Security guards and ID badges
- Video surveillance (CCTV)
- Mantraps and biometric scanners
- Fire suppression and environmental controls (HVAC)

Purpose: To protect physical infrastructure and prevent unauthorized hands-on access.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Categories)

Control Type	What It Is	Primary Purpose	Examples
Administrative	Policies, procedures, human factors	Manage people and process behavior	Training, hiring policies, audits
Technical (Logical)	Systems and software controls	Protect data and systems digitally	Firewalls, encryption, access control
Physical	Tangible, real-world barriers	Secure physical spaces	Locks, guards, cameras

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Types)

These are the functional types of security controls—classified by what they do to manage risk.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Types)

These are the functional types of security controls—classified by what they do to manage risk.

Preventive Controls

Examples:

- Firewalls blocking unauthorized traffic
- Security awareness training
- Locked doors and access controls
- Encryption (prevents data theft even if stolen)

Purpose: Stop security incidents before they happen.

No matter what you do, you will NOT be able to stop ALL bad things from happening.

Therefore, you MUST be able to DETECT the things you couldn't prevent.

AND have a plan in place to RESPOND.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Types)

These are the functional types of security controls—classified by what they do to manage risk.

Detective Controls

Examples:

- Intrusion detection systems (IDS)
- Security cameras and motion detectors
- Log monitoring and SIEM alerts
- File integrity monitoring

Purpose: Identify and alert when a security incident has occurred or is in progress.

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Types)

These are the functional types of security controls—classified by what they do to manage risk.

Corrective Controls

Examples:

- Antivirus software removing malware
- Patching vulnerabilities
- Reimaging a compromised system
- Access control changes after a breach

Purpose: Fix or restore systems after a security incident is detected.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Types)

These are the functional types of security controls—classified by what they do to manage risk.

Recovery Controls

Examples:

- Backups and restoration processes
- Disaster recovery plans (DRP)
- Alternate sites or failover systems
- Business continuity plans

Purpose: Bring systems and data back to normal operations after a serious incident or disaster.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Types)

These are the functional types of security controls—classified by what they do to manage risk.

Deterrent Controls

Examples:

- Warning signs and security banners
- Visible cameras or guards
- Legal and HR policy notices
- “This area under surveillance” alerts

Purpose: Discourage or dissuade potential attackers or malicious insiders.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Types)

These are the functional types of security controls—classified by what they do to manage risk.

Directive Controls

Examples:

- Security policies and acceptable use agreements
- Standard operating procedures (SOPs)
- Mandatory security training
- Code of conduct documents

Purpose: Guide behavior or enforce specific actions, usually through policies or procedures.

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Types)

These are the functional types of security controls—classified by what they do to manage risk.

Compensating Controls

Examples:

- Manual log reviews if SIEM isn’t available
- Physical access logs if biometric access isn’t possible
- Increased monitoring if patching is delayed
- MFA used to compensate for weak passwords

Purpose: Provide alternate protection when the ideal control is not feasible, due to cost or limitations.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Countermeasure Selection and Implementation (Types)

Control Type	Primary Purpose	Example
Preventive	Block or stop unwanted activity	Firewalls, encryption, access control
Detective	Identify and alert on suspicious activity	IDS, SIEM alerts, video surveillance
Corrective	Fix problems after detection	Antivirus removal, patching
Recovery	Restore systems and data	Backups, disaster recovery plans
Deterrent	Dissuade malicious behavior	Warning signs, visible cameras
Directive	Enforce proper behavior through instruction	Policies, training, procedures
Compensating	Alternative when primary control isn't possible	Manual reviews, extra monitoring

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Risk Reporting and Documentation

Risk Reporting – the process of communicating identified risks, their potential impact, and mitigation efforts to key stakeholders to support informed decision-making and ongoing risk management.

- **Internal Reporting**
  - Sharing risk information within the organization—typically with executives, business units, IT, and security teams—to align risk priorities, actions, and accountability.
  - Example: Monthly security risk dashboard sent to senior leadership.
- **External Reporting**
  - Providing risk-related information to outside parties, such as regulators, auditors, insurers, or customers, to meet compliance requirements, maintain transparency, or fulfill contractual obligations.
  - Example: Sharing risk assessment results with a third-party auditor or regulator.

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Other Common Terms:

- **Risk register** - a centralized document or tool used to track, assess, and manage identified information security risks, including their status, impact, likelihood, and mitigation plans.
- **Enterprise Risk Management (ERM)** - a holistic approach to identifying, assessing, and managing all types of risks—including information security risks—across an entire organization to support strategic objectives.
- **Risk Maturity Model (RMM)** - a framework that helps organizations measure how well they identify, assess, manage, and respond to risks—and shows them how to improve over time.
- **Inherent risk** - the level of risk that exists before any controls or safeguards are applied in an information security context.
- **Residual risk** - the remaining risk after security controls and safeguards have been implemented.
- **Legacy risk** - the risk associated with outdated or unsupported systems, software, or processes that may no longer meet current security standards.

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Risk Frameworks

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Risk Frameworks

Cybersecurity Framework (CSF) 2.0

CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Risk Frameworks

Cybersecurity Framework (CSF) 2.0

- Developed by NIST (National Institute of Standards and Technology)
- Flexible, risk-based approach to help organizations manage and improve their cybersecurity posture, regardless of size, sector, or maturity level
- Organized around six key **Functions**, which represent high-level cybersecurity outcomes:
    1. **Govern** (new in 2.0) – Establish organizational context, roles, and risk management strategies.
    2. **Identify** – Understand assets, systems, data, and risks.
    3. **Protect** – Safeguard assets with controls and procedures.
    4. **Detect** – Identify cybersecurity events promptly.
    5. **Respond** – Take action against detected cybersecurity incidents.
    6. **Recover** – Restore normal operations and resilience after incidents.

Each Function is broken down into Categories and Subcategories that describe specific outcomes and activities (e.g., access control, incident response, supply chain risk management).

2025 CISSP MENTOR PROGRAM

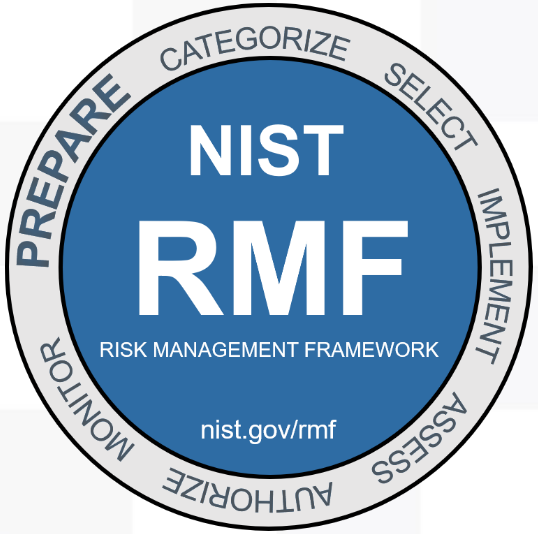
CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Risk Frameworks

Risk Management Framework (RMF) (defined by NIST in SP 800-37 Rev. 2)



CHAPTER 2

Personnel Security and Risk Management Concepts

Understand and Apply Risk Management Concepts

Risk Frameworks

CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
PREPARE
NIST
RMF
RISK MANAGEMENT FRAMEWORK
nist.gov/rmf

Risk Management Framework (RMF) (defined by NIST in SP 800-37 Rev. 2)

- A structured, flexible, and repeatable process for managing information security and privacy risk
- The 7 Steps of the RMF:
  1. **Prepare** (new in Rev. 2) - Establish context, assign roles, and get the organization ready to manage risk.
  2. **Categorize** - Define the system and classify it based on the potential impact of a breach (confidentiality, integrity, availability).
  3. **Select** - Choose appropriate security and privacy controls based on the system's categorization (often from NIST SP 800-53).
  4. **Implement** - Deploy the selected controls and document how they are applied.
  5. **Assess** - Evaluate whether the controls are implemented correctly, operating as intended, and producing the desired results.
  6. **Authorize** - A senior official formally accepts the risk and approves the system for operation.
  7. **Monitor** - Continuously observe controls, track risk, and update as the system or environment changes.

Why It's Important:

- Required for U.S. federal systems and widely adopted across public and private sectors
- Supports continuous authorization, risk-based decisions, and compliance
- Aligns with other frameworks like NIST CSF, ISO 27001, and FedRAMP

CHAPTER 2

Personnel Security and Risk Management Concepts

Social Engineering

A manipulation technique where attackers **exploit human trust**, **emotions, or behavior** to trick individuals into revealing confidential information or performing actions that compromise security—often bypassing technical controls entirely.

- In Simple Terms: It's hacking people, not systems.
- Common Social Engineering Tactics:
  - **Phishing**: Fake emails that trick users into clicking malicious links or giving up credentials
  - **Pretexting**: Using a made-up story to gain trust or access
  - **Baiting**: Offering something tempting (like a free USB drive or download) to lure a victim
  - **Tailgating**: Following someone into a secure area by pretending to belong
  - **Vishing**: Voice phishing via phone calls pretending to be from trusted sources

Why It's Dangerous:
Even the best technology can't stop a user who's convinced to hand over their password or click the wrong link. That's why security awareness training and a strong security culture are essential.

CHAPTER 2

Personnel Security and Risk Management Concepts

Social Engineering

These principles are often combined for maximum effect—like a fake CEO (authority) demanding urgent (urgency) action to approve a payment (trust).

Social Engineering Principles

- **Authority** - Attackers pretend to be someone in power (e.g., a boss, law enforcement, or IT admin) to pressure the victim into compliance.
- **Intimidation** - Uses threats or fear to scare the victim into acting quickly—often combined with authority.
- **Consensus** (Social Proof) - Relies on the idea that if others are doing it, it must be safe or acceptable (e.g., “Everyone’s updated their credentials—have you?”).
- **Scarcity** - Creates a sense of limited time or availability to push people into quick decisions (e.g., “Only the first 50 people get this bonus!”).
- **Familiarity** - The attacker builds a rapport by pretending to be someone the victim knows or relates to, like a coworker, friend, or vendor.
- **Trust** - Exploits the victim’s belief that the attacker or message comes from a reliable, safe source, such as a well-known brand or IT department.
- **Urgency** - Forces the victim to act quickly without thinking, often by inventing emergencies or tight deadlines (e.g., “Your account will be locked in 10 minutes!”).

CHAPTER 2

Personnel Security and Risk Management Concepts

Social Engineering

Common Methods

- **Phishing**
  - Description: Fraudulent emails trick users into clicking malicious links or giving up credentials.
  - Example: An email pretending to be from Microsoft asking you to “reset your password.”
- **Smishing**
  - Description: Phishing via SMS text messages.
  - Example: “Your bank account is locked. Tap this link to verify your identity.”
- **Vishing**
  - Description: Phishing attacks via voice calls.
  - Example: A caller claims to be from the IRS demanding payment with threats of arrest.
- **Spear Phishing**
  - Description: Targeted phishing aimed at a specific individual or role.
  - Example: An attacker sends a fake invoice to a company’s accounts payable clerk.

CHAPTER 2

Personnel Security and Risk Management Concepts

Social Engineering

Common Methods

- **Whaling**
  - Description: Spear phishing that targets high-value targets.
  - Example: A fake email to the CFO asking for urgent wire transfer approval.
- **Spam**
  - Description: Unsolicited, often irrelevant emails—can be annoying or malicious.
  - Example: Mass marketing emails with sketchy attachments or links.
- **Shoulder Surfing**
  - Description: Watching over someone’s shoulder to steal sensitive information.
  - Example: Observing someone enter a PIN at an ATM or password at a login screen.
- **Invoice Scams**
  - Description: Fake invoices sent to trick companies into paying non-existent bills.
  - Example: An attacker sends a “renewal invoice” for a software license no one ordered.

CHAPTER 2

Personnel Security and Risk Management Concepts

Social Engineering

Common Methods

- **Hoax**
  - Description: A false warning or message designed to cause fear, distraction, or wasted effort.
  - Example: An email saying “Your account will be deleted unless you act now!” when it’s fake.
- **Impersonation / Masquerading**
  - Description: Pretending to be someone trusted to gain access or information.
  - Example: An attacker poses as IT support to ask for your password.
- **Tailgating / Piggybacking**
  - Description: Gaining physical access by following someone into a secure area.
  - Example: An attacker walks in behind an employee holding the door open.
- **Baiting**
  - Description: Offering something tempting to trick victims into downloading malware.
  - Example: A USB drive labeled “Salary Info” left in a parking lot, loaded with malware.

CHAPTER 2

Personnel Security and Risk Management Concepts

Social Engineering

Common Methods

- **Dumpster Diving**
  - Description: Searching through physical trash to find sensitive documents or data.
  - Example: Finding discarded printouts with usernames, passwords, or account numbers.
- **Typosquatting**
  - Description: Registering misspelled domain names to trick users into visiting fake sites.
  - Example: Users visit “amaz0n.com” thinking it’s Amazon and get phished.
- **Influence Campaigns**
  - Description: Coordinated efforts to manipulate public opinion or spread misinformation.
  - Example: Fake social media accounts spreading false election info or divisive content.
- **Hybrid Warfare**
  - Description: Combining cyberattacks, misinformation, and physical tactics to destabilize a target—often used by nation-states.
  - Example: A country disrupts another’s infrastructure while flooding media with propaganda and launching phishing campaigns..

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Social Engineering

Common Methods

- **Dumpster Diving**
  - Description: Searching through physical trash to find sensitive documents or data.
  - Example: Finding di
- **Typosquatting**
  - Description: Registe
  - Example: Users visit
- **Influence Campaigns**
  - Description: Coordinated efforts to manipulate public opinion or spread misinformation.
  - Example: Fake social media accounts spreading false election info or divisive content.
- **Hybrid Warfare**
  - Description: Combining cyberattacks, misinformation, and physical tactics to destabilize a target—often used by nation-states.
  - Example: A country disrupts another's infrastructure while flooding media with propaganda and launching phishing campaigns..

Business Email Compromise (BEC)

- Description: A targeted social engineering attack where cybercriminals spoof or take over a legitimate business email account to trick employees into sending money, credentials, or sensitive data.
- Example: An attacker compromises the CEO's email and sends a realistic request to the finance team: "Please process a $75,000 wire transfer to this vendor today—very urgent and confidential."

2025 CISSP MENTOR PROGRAM

CHAPTER 2

Personnel Security and Risk Management Concepts

Establish and Maintain a Security Awareness, Education, and Training Program

CHAPTER 2

Personnel Security and Risk Management Concepts

Establish and Maintain a Security Awareness, Education, and Training Program

The best programs are ones that are relevant and clearly answer “What’s in it for me?”

Definitions

Term	Definition
Awareness	Focuses on **shaping attitudes and behaviors** by making people aware of risks and their role in security.
Training	Provides people with **specific skills** to perform their job securely.
Education	Offers a **deep understanding of security concepts**, often in a formal, academic, or career-development setting.

CHAPTER 2

Personnel Security and Risk Management Concepts

Establish and Maintain a Security Awareness, Education, and Training Program

The best programs are ones that are relevant and clearly answer “What’s in it for me?”

Key Differences

	Awareness	Training	Education
Goal	Influence behavior	Build job-specific skills	Build foundational knowledge
Depth	Broad and general	Focused and task-based	In-depth and often theoretical
Format	Posters, emails, reminders	Hands-on sessions, exercises	Courses, degrees, certifications
Audience	Everyone in the organization	Specific roles or departments	Security professionals or students

CHAPTER 2

Personnel Security and Risk Management Concepts

Establish and Maintain a Security Awareness, Education, and Training Program

The best programs are ones that are relevant and clearly answer “What’s in it for me?”

Examples

Awareness:

- A poster in the office saying, “Think before you click—phishing emails are everywhere!”
- A quick video reminder during Cybersecurity Awareness Month

Training:

- Teaching help desk staff how to reset passwords securely
- A hands-on session for employees on how to spot a phishing email in Outlook

Education:

- Enrolling in a CISSP course or university program on cybersecurity
- Learning cryptographic principles in a formal classroom setting

CHAPTER 2

Personnel Security and Risk Management Concepts

Establish and Maintain a Security Awareness, Education, and Training Program

The best programs are ones that are relevant and clearly answer “What’s in it for me?”

Why All Three Matter:

- Awareness helps people care
- Training helps people act
- Education helps people understand

Together, they build a culture of security and empower your workforce to defend against threats.

- Learning cryptographic princip

It’s always a good idea to determine/measure the effectiveness of these programs through exercises, tests, quizzes, surveys, etc.

2025 CISSP MENTOR PROGRAM

YAY! YOU MADE IT!

That was A LOT of information.

2025 CISSP MENTOR PROGRAM

YAY! YOU MADE IT!

That was A LOT of information.

Now what?

- Keep up in the book. We just went through all of Chapter 1 and Chapter 2.
- Be sure to review and focus on the “Study Essentials” sections for each chapter.
- If you’re ambitious, do the “Written Lab” section for each chapter too.
- When you’re ready, take a stab at the “Review Questions” for each chapter.
- Jot down your questions, post them in Discord, and/or ask them in the next Live Mentor Session (April 30th)

That’s it for now, **CONGRATS** for making it through this. ☺

See you Wednesday night.