Cybersecurity Fundamentals

Module 1 : Security Principles

Security Principles

Security Concepts

Risk Management Process

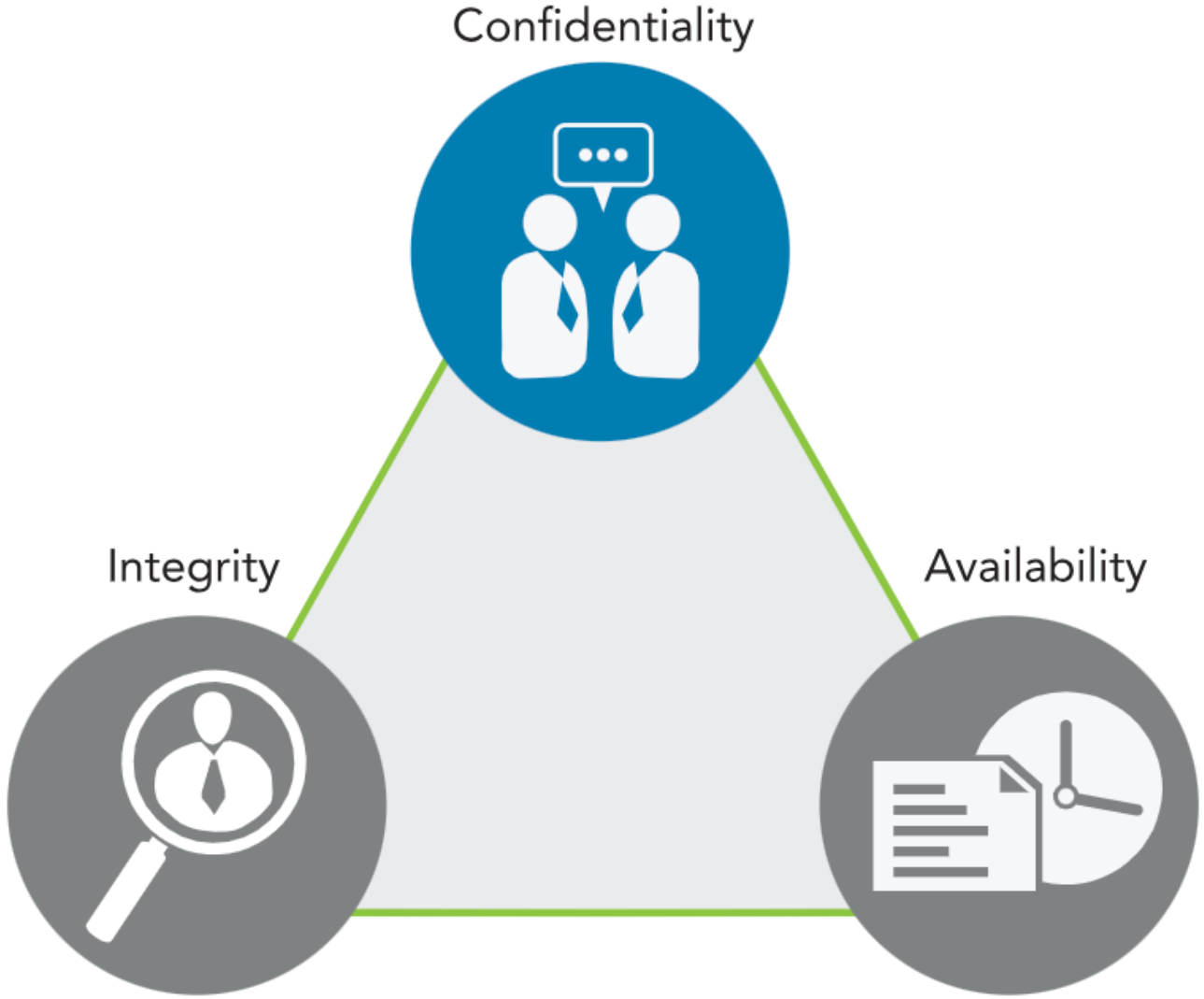
Security Controls

Governance Elements and Process

Security Concepts

- The CIA Triad
- CIA Triad Deep Dive
- Authentication
- Methods of Authentication
- Non-repudiation
- Privacy

Security Concepts : The CIA Triad



Security Concepts : CIA Triad Deep Dive

Confidentiality
Confidentiality relates to permitting authorized access to information, while at the same time protecting information from improper disclosure.

Personally Identifiable Information (PII)
protected health information (PHI)
classified or sensitive information
sensitivity

Integrity
Integrity is the property of information whereby it is recorded, used and maintained in a way that ensures its completeness, accuracy, internal consistency and usefulness for a stated purpose.

information or data
systems and processes for business operations
organizations
people and their actions
Data Integrity
System Integrity (state & baseline)

Availability
Availability means that systems and data are accessible at the time users need them.

criticality

Security Concepts : Authentication

This process of verifying or proving the user's identification is known as authentication. Simply put, authentication is a process to prove the identity of the requestor.

There are three common methods of authentication:

Something you know: Passwords or passphrases	Something you have: Tokens, memory cards, smart cards	Something you are: **Biometrics** , measurable characteristics

Security Concepts : Methods of Authentication

- Single-factor authentication
- Multi-factor authentication
- Common best practice is to implement at least two of the three common techniques for authentication:
  - Knowledge-based
  - Token-based
  - Characteristic-based

Security Concepts : Non-repudiation

Protection against an individual falsely denying having performed a particular action.

Non-repudiation methodologies ensure that people are held responsible for transactions they conducted.

Security Concepts : Privacy

The right of an individual to control the distribution of information about themselves.

General Data Protection Regulation (GDPR)

Security Concepts : Summary

Authorization	*The right or a permission that is granted to a system entity to access a system resource.*
Integrity	*The property that data has not been altered in an unauthorized manner.*
Confidentiality	*The characteristic of data or information when it is not made available or disclosed to unauthorized persons or processes.*
Privacy	*The right of an individual to control the distribution of information about themselves.*
Availability	*Ensuring timely and reliable access to and use of information by authorized users.*
Non-repudiation	*The inability to deny taking an action, such as sending an email message.*
Authentication	*Access control process that compares one or more factors of identification to validate that the identity claimed by a user or entity is known to the system.*

Risk Management Process : Risk Management Terminology

Asset : something in need of protection.

Vulnerability : a gap or weakness in those protection efforts.

Threat : something or someone that aims to exploit a vulnerability to thwart protection efforts.

RISK MANAGEMENT PROCESS : RISK IDENTIFICATION

a recurring process of identifying different possible risks, characterizing them and then estimating their potential for disrupting the organization.

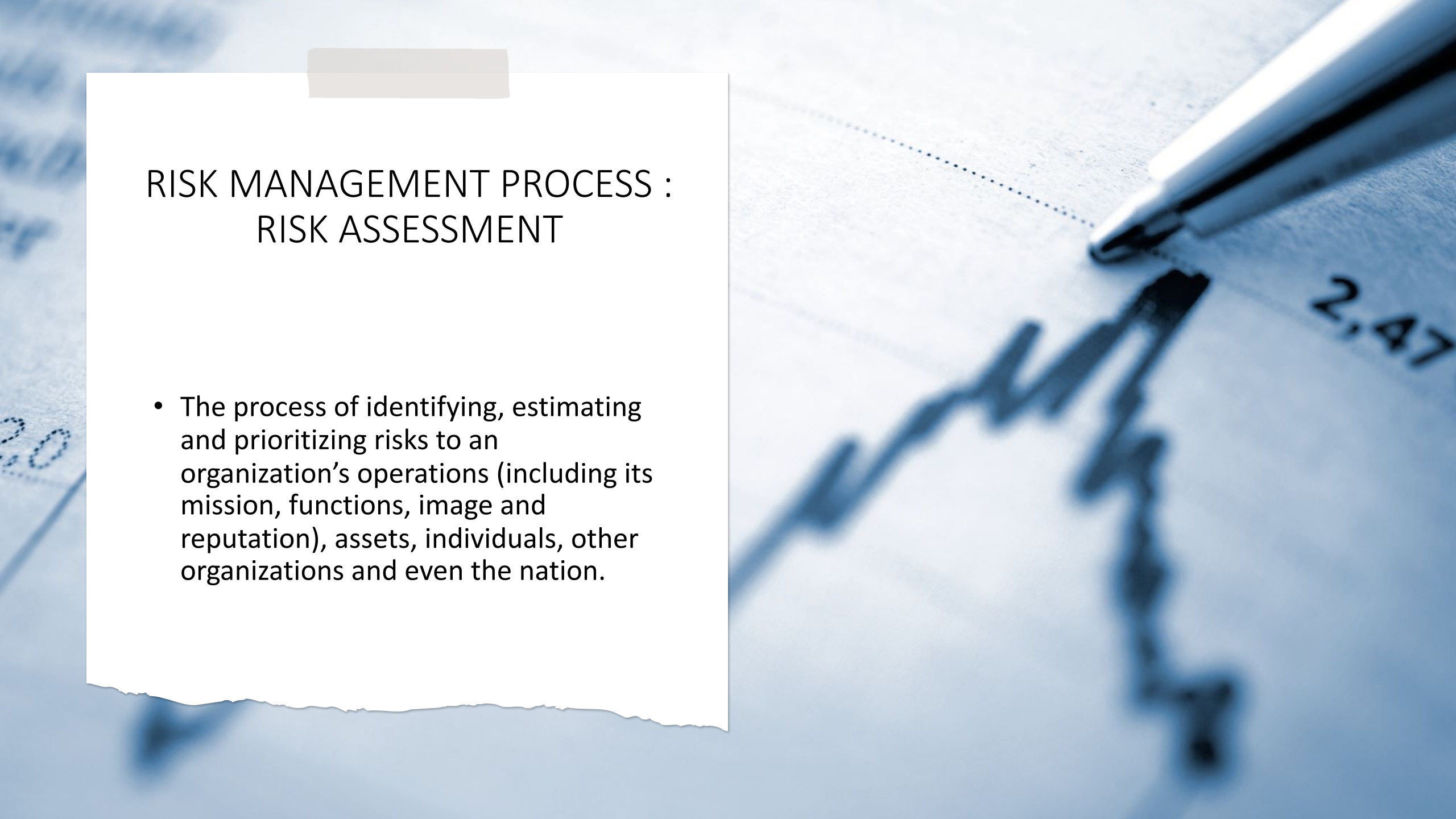
Identify risk to communicate it clearly.

Employees at all levels of the organization are responsible for identifying risk.

Identify risk to protect against it.

RISK MANAGEMENT PROCESS : RISK ASSESSMENT

- The process of identifying, estimating and prioritizing risks to an organization’s operations (including its mission, functions, image and reputation), assets, individuals, other organizations and even the nation.

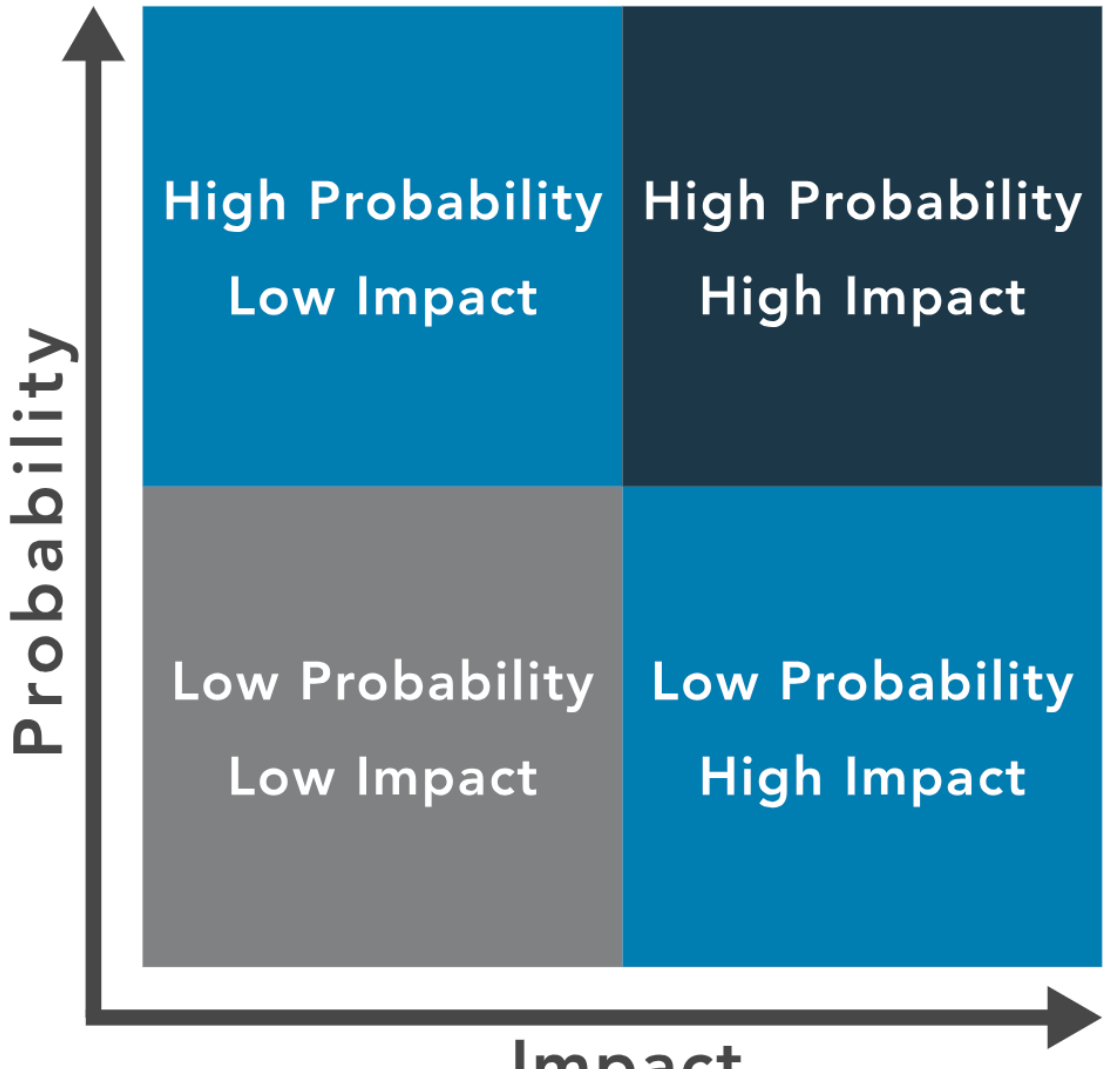


RISK MANAGEMENT PROCESS : RISK TREATMENT

- Risk avoidance is the decision to attempt to eliminate the risk entirely.
- Risk mitigation is taking actions to prevent or reduce the possibility of a risk event or its impact.
- Risk transference is the practice of passing the risk to another party, who will accept the financial impact of the harm resulting from a risk being realized in exchange for payment.
- Risk acceptance is taking no action to reduce the likelihood of a risk occurring.

RISK MANAGEMENT PROCESS : RISK PRIORITIES

- Qualitative risk analysis
- Quantitative risk analysis

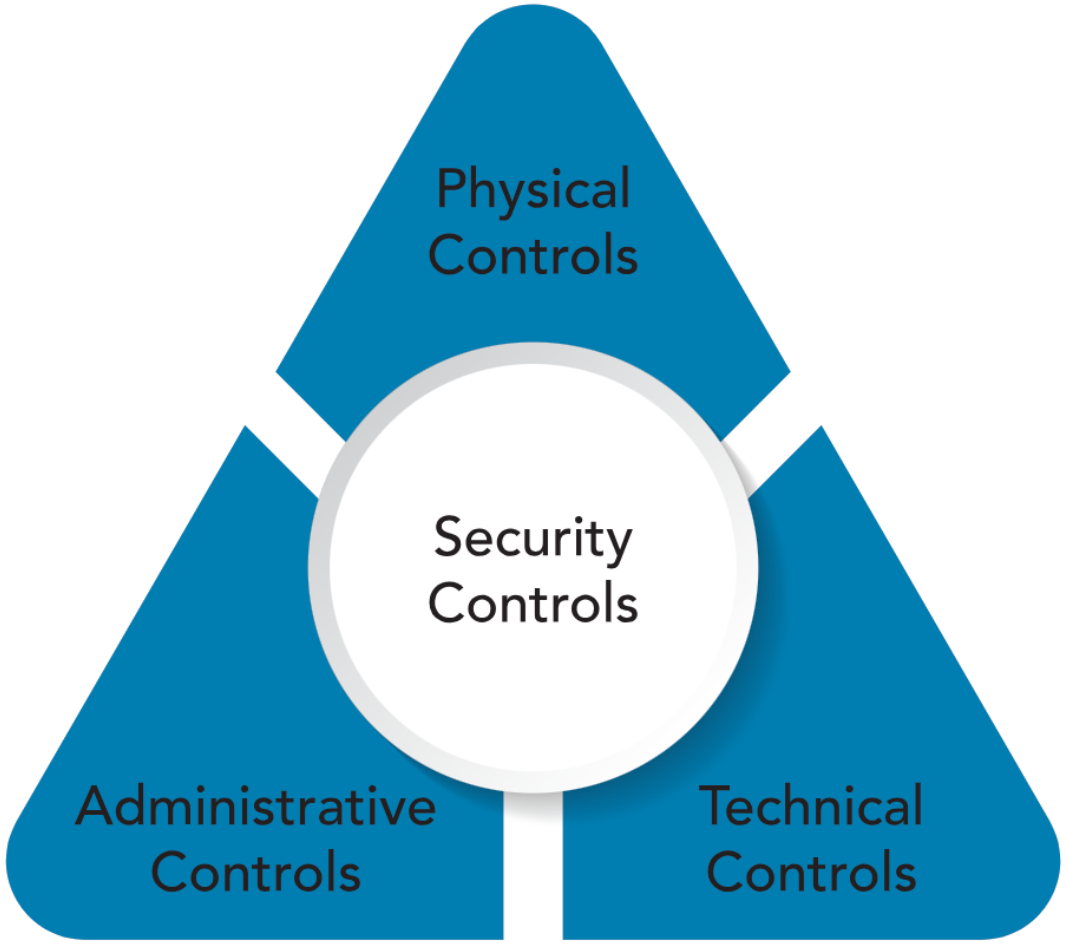


Risk Term Review

Mitigation	*Taking action to prevent or reduce the impact of an event.*
Acceptance	*Ignoring the risks and continuing risky activities.*
Avoidance	*Ceasing the risky activity to remove the likelihood that an event will occur.*
Vulnerability	*An inherent weakness or flaw.*
Asset	*Something of value that is owned by an organization, including physical hardware and intellectual property.*
Threat	*A person or entity that deliberately takes action to exploit a target.*
Transference	*Passing risk to a third party.*

SECURITY CONTROL : WHAT IS SECURITY CONTROL?

- Security controls pertain to the physical, technical and administrative mechanisms that act as safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information.
- The implementation of controls should reduce risk, hopefully to an acceptable level.



SECURITY CONTROL : PHYSICAL CONTROL

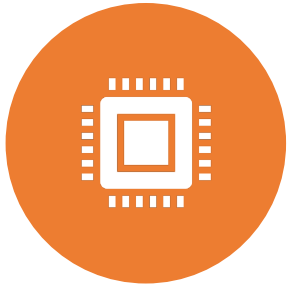
Physical controls address process-based security needs using physical hardware devices, such as badge readers, architectural features of buildings and facilities, and specific security actions to be taken by people.

Controlling, directing or preventing the movement of people and equipment throughout a specific physical location

Protection and control over entry onto the land surrounding the buildings, parking lots or other areas that are within the organization’s control

Physical controls are supported by technical controls as a means of incorporating them into an overall security system.

SECURITY CONTROL : TECHNICAL CONTROL



Security controls that computer systems and networks directly implement.

Provide automated protection from unauthorized access or misuse.

Facilitate detection of security violations

Support security requirements for applications and data.

SECURITY CONTROL : ADMINISTRATIVE CONTROL

Directives, guidelines or advisories aimed at the people within the organization

Provide frameworks, constraints and standards for human behavior

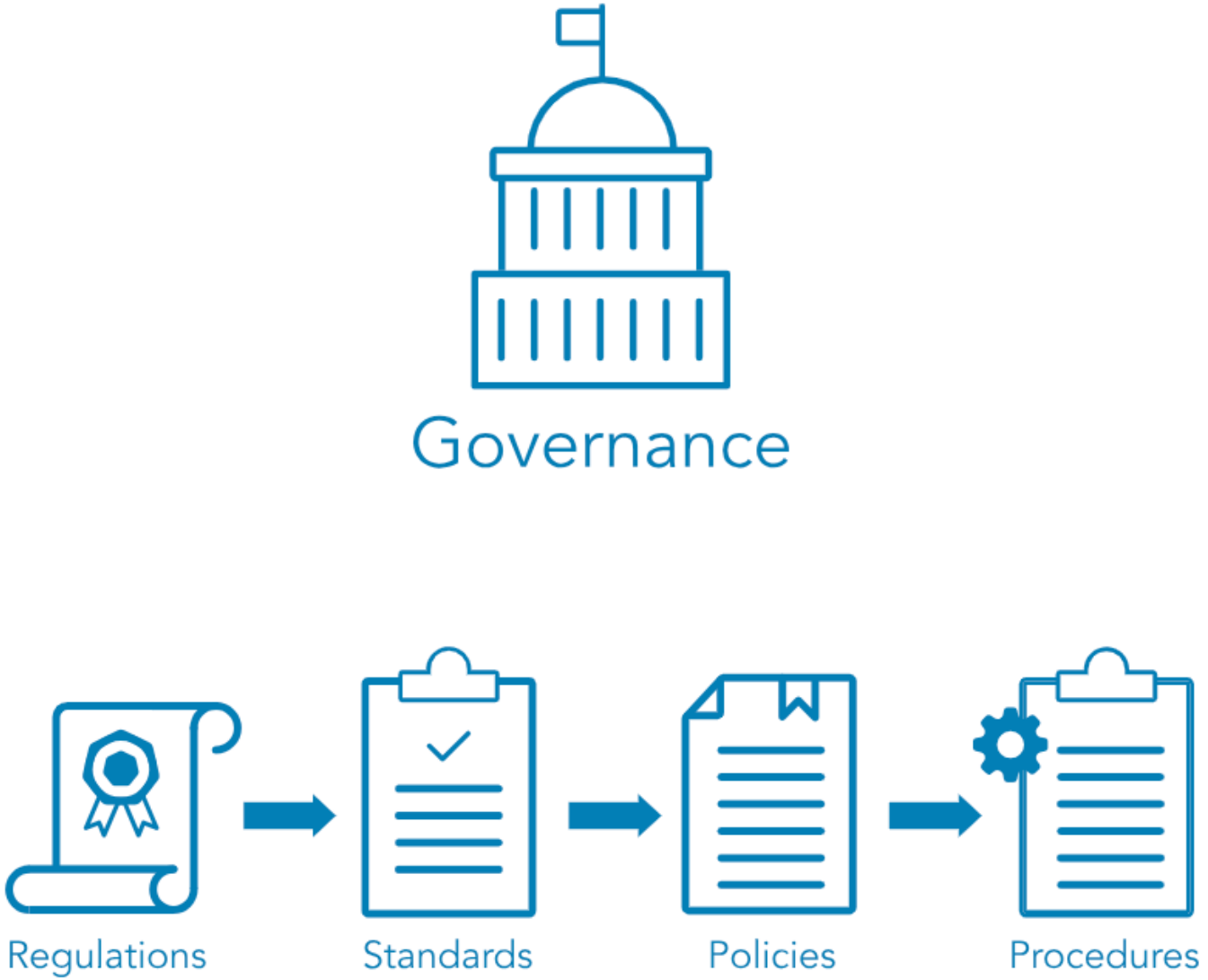
Cover the entire scope of the organization’s activities and its interactions

- External parties
- Stakeholders

GOVERNANCE ELEMENTS

- REGULATIONS
  - commonly issued in the form of laws, usually from government (not to be confused with governance) and typically carry financial penalties for noncompliance.
- STANDARD
  - provide a framework to introduce policies and procedures in support of regulations.
- POLICIES
  - guidance in all activities to ensure that the organization supports industry standards and regulations.
- PROCEDURES
  - detailed steps to complete a task that support departmental or organizational policies.

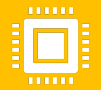
GOVERNANCE PROCESS



STANDARDS

The International Organization for Standardization (ISO) develops and publishes international standards on a variety of technical subjects, including information systems and information security, as well as encryption standards. ISO solicits input from the international community of experts to provide input on its standards prior to publishing.

The National Institute of Standards and Technology (NIST) is a United States government agency under the Department of Commerce and publishes a variety of technical standards in addition to information technology and information security standards. Many of the standards issued by NIST are requirements for U.S. government agencies and are considered recommended standards by industries worldwide.



From Internet Engineering Task Force (IETF), there are standards in communication protocols that ensure all computers can connect with each other across borders, even when the operators do not speak the same language.

The Institute of Electrical and Electronics Engineers (IEEE) also sets standards for telecommunications, computer engineering and similar disciplines.