Domain 1: Security Principles

▼ Safeguarding Data

Concepts Covered:

- The Confidentiality, Integrity, and Availability (CIA) Triad
- CIA Triad Deep Dive
- CIA in Real world
- Non-repudiation
- Protecting Information
- Making Connections

1. The CIA Triad: Introduction

The **CIA Triad**—Confidentiality, Integrity, and Availability—is a foundational model in information security. Its purpose is to use relevant terms to clarify and define security's aims, making the concept accessible to management, users, and security professionals.

- **Confidentiality:** Ensures only authorized individuals have access to information, protecting it from improper disclosure.
- **Integrity:** Ensures information is complete, accurate, consistent, and useful by protecting it from unauthorized changes.
- **Availability:** Ensures systems and data are accessible to authorized users whenever needed.

2. Deep Dive into CIA Triad Elements

Confidentiality

- **Meaning:** Only those authorized can access specific information; protection from leaks or exposure to unauthorized parties.

- **Challenges:** In environments with numerous guest users or unknown devices, like public web apps, maintaining confidentiality is complex.
- **Key Terms:**
  - **PII (Personally Identifiable Information):** Data that could identify an individual (e.g., name + date of birth).
  - **PHI (Protected Health Information):** Health-related data tied to individuals.
  - **Classified/Sensitive Information:** Includes trade secrets, intellectual property, or business plans.
  - **Sensitivity:** The level of importance or need for protection assigned to particular data.
- **Example:** A hospital must protect patient names, birth dates, and medical records from unauthorized access.

Integrity

- **Meaning:** Ensures information remains whole, correct, and consistent across its lifecycle—storage, processing, and transmission.
- **Applies To:**
  - **Data:** Must not be altered without authorization; should remain complete and accurate.
  - **Systems/Processes:** Must function as expected, without unauthorized changes.
  - **People/Organizations:** Should act consistently and reliably.
- **Data Integrity:** Protects against unauthorized modifications, errors, and data loss—integrity applies to data in storage, processing, and transit.
- **System Integrity:** Maintains systems in a known, trusted state (baseline), checking for unauthorized changes.
- **Legal Drivers:** Regulations may require organizations to safeguard the integrity of certain data.

- **Example:** Changing a patient's drug allergy information in a health records system without proper authorization can cause severe harm.

Availability

- **Meaning:** Ensures information and resources are accessible and usable when needed by authorized users, in the required form.
- **Not Absolute:** 100% uptime is not always necessary, but must meet business needs.
- **Criticality:** Some data or systems are more vital; their availability becomes a business priority.
- **Mitigation:** Identify critical systems with the business to ensure their availability meets required levels.
- **Example:** Banking systems must remain accessible so customers and staff can perform transactions without disruption.

3. The CIA Triad in Real-World Contexts

- **Confidentiality:** Vital in industries like banking, insurance, and healthcare, where a breach means exposing sensitive, personal, or financial information.
- **Integrity:** Prevents unauthorized changes—vital for accurate health records, financial transactions, or business operations. Breaches can lead to severe consequences such as improper patient care due to modified records.
- **Availability:** Key for business continuity. For example, ransomware attacks can cripple access, halting business operations and services until the issue is resolved. Without timely access to data and services, businesses may lose reputation and customers.

4. Non-Repudiation

- **Definition:** Prevents anyone involved in a transaction or communication from denying their participation or the action they performed.

- **Legal Relevance:** Ensures parties cannot plausibly deny sending/receiving messages, approving actions, or creating/altering information.
- **Modern Context:** Crucial in e-commerce and electronic transactions to ensure trust and responsibility. Tools such as digital signatures and transaction logs help establish non-repudiation.
- **Example:** If someone makes an online purchase, non-repudiation mechanisms prevent them from later denying the transaction.

5. Protecting Information: The Role of PII

- **PII is Contextual:** Some data elements (e.g., a date of birth) may not identify a person alone but become sensitive when combined with other elements (like name or address).
- **Security Professional's Role:** Responsible for identifying and protecting all forms of sensitive and personal data. This applies to both organizational and customer information.
- **Everyday Relevance:** Whether you're receiving medical care, banking, or using email, the protection of your information underpins trust and safety.
- **Developing Security Thinking:** Security professionals must develop a mindset focused on pre-emptive protection of information in various contexts.

6. Threats and Risk Examples to CIA Triad

- **Human Errors:** Sharing passwords (intentionally or not) can undermine confidentiality (unauthorized access) and integrity (unauthorized changes).
    - *Example:* Joe shares his password with Joanne, allowing her ongoing access even after her credentials are revoked.
- **Physical Security Lapses:** Leaving workstations unlocked or unattended can allow family members or others to introduce malware or corrupt software, compromising integrity and possibly confidentiality.
- **Environmental Threats:** Natural disasters (e.g., extended power outages) can disable backup systems, impacting availability; poor fire suppression

can destroy both digital and analog records, harming all triad elements.

- **Malicious Acts:** Disgruntled employees using acquired credentials for sabotage, introducing malware, or deleting information.
- **Lesson:** Organizations must perform comprehensive risk assessments encompassing technical, human, and environmental vectors and implement effective mitigation measures.

Summary Table: CIA Triad & Associated Concepts

Concept	Definition	Examples	Common Threats
Confidentiality	Only authorized access to information; protect from disclosure.	Protecting medical records, financial data	Unauthorized access, phishing
Integrity	Assurance information is unaltered, consistent, and correct across its lifecycle.	Transaction logs, system baselining, checksums	Insider abuse, malware
Availability	Ensuring data/systems are accessible when needed by authorized users.	Online banking systems, healthcare systems	DDoS attacks, hardware failure
Non-repudiation	Preventing denial of individual actions or transactions.	Digital signatures on transactions	Weak authentication
PII Protection	Identifying/protecting combinations of personal data that uniquely identify individuals	Name + birthdate + address, Social Security Numbers	Data aggregation, breaches

▼ Identity Assurance

Concepts Covered:

- Authentication
- Methods of Authentication
- Proving Identity

- Risk in our Lives
- Professional Code of Conduct
- Theoretical Example: Code of Ethics

---

1. Authentication

Definition

Authentication is the process of verifying that a user (or requestor) is truly who they claim to be. It is essential for ensuring confidentiality and protecting sensitive data and resources.

Purpose

- Validates if a given identity actually belongs to the requestor.
- Prevents unauthorized access to systems and information.

Methods of Authentication

Authentication is generally based on at least one of the following three categories:

1. **Something you know**
    - Examples: Passwords, passphrases, personal identification numbers (PINs).
    - **Use case:** Entering a password to log into an online account.
2. **Something you have**
    - Examples: Security tokens, memory cards, smart cards.
    - **Use case:** Swiping an access card to enter a secure office area.
3. **Something you are**
    - Examples: Biometric data such as fingerprints, facial recognition, iris scans.
    - **Use case:** Unlocking a phone with your fingerprint.

2. Methods of Authentication

Single-Factor Authentication (SFA)

- Only one method (from the above three) is used.
- **Example:** Logging in with just a password.

Multi-Factor Authentication (MFA)

- Requires two or more different factors from the three categories.
- Significantly increases security by combining different evidences of identity.
- **Example:** Logging in with a password (something you know) and a one-time code sent to your phone (something you have).

Subtypes of Authentication

1. **Knowledge-Based Authentication**
    - Relies on information only the user should know (e.g., password or PIN).
    - *Risk:* Vulnerable to social engineering or reset attacks.
2. **Token-Based Authentication**
    - Utilizes physical tokens like smart cards or USB keys.
    - Often used for strong access control.
3. **Characteristic-Based Authentication**
    - Relies on biological traits (e.g., fingerprints, voice, retina).
    - *Risk:* Can present privacy concerns and potential for spoofing.

Security Recommendation

- Best practice: Use at least two of the three factors for sensitive or critical systems.
- Note: Using two knowledge-based credentials (like user ID and password) is **not** considered true MFA.

3. Proving Identity: Real-World Examples

- Authenticating identity is often a layered process of combining factors.
- **Bank ATM Example:**
  - Card (something you have) + PIN (something you know) = MFA.
  - Possession of one factor without the other does not allow access.
- **Biometrics:**
  - Increasingly used as an additional layer (e.g., fingerprint to unlock devices).
- Everyday systems (like smartphone login, online banking) now commonly use multi-factor authentication for improved security.

4. Risk in Our Lives

Everyday Risks and Impacts

- **Example:** Unauthorized credit card charges.
  - Storing card info on devices may be convenient but increases risk.
  - Banks may protect from charges, but you'll deal with account freezes and replacement hassles.

Risk Mitigation Strategies

- **Layered Security:** Adding MFA for online banking, so theft of your password alone doesn't compromise your account.
- **Insurance:** Transferring financial risk by purchasing travel, health, or identity theft insurance.
  - *Example:* Buying travel insurance to protect prepaid expenses against unforeseen trip cancellations.
- **Identity Theft Protection:** Some companies insure against identity theft, evaluating payouts versus customer premiums.

General Principle

- **Identification and management of risks**—either by adding security controls or by transferring risk via insurance—are fundamental in day-to-day life and professional settings.

5. Professional Code of Conduct

ISC2 Code of Ethics Overview

- ISC2-certified information security professionals are held to high ethical standards.
- Adherence to the **Code of Ethics** is both a privilege and a requirement.

Preamble

- Stresses the protection of society, common good, and necessitates the highest ethical standards.
- Compliance is mandatory for certification holders.

Four Canons of the ISC2 Code of Ethics

1. **Protect society, the common good, public trust, and critical infrastructure.**
2. **Act honorably, honestly, justly, responsibly, and legally.**
3. **Provide diligent and competent service to principals.**
4. **Advance and protect the profession.**

Summary: Adhering to these canons means being responsible not just for technical excellence, but also for maintaining trust and ethical integrity in all actions.

6. Theoretical Example: Code of Ethics in Practice

Example 1: Misuse of Sensitive Biometrics

- An organization used retinal scans not only for access but also to determine gender and pregnancy—then discriminated in hiring.

- Such use violates the ethical canon requiring security professionals to act “honorably, honestly, justly, responsibly, and legally.”
    - *Key Point:* Gathering and misapplying sensitive information for discrimination is unethical and likely illegal.

Example 2: Abuse of Authority and Monitoring

- A network admin, not assigned to monitor a user, intervenes due to a personal conflict.
- Investigation found the admin used his privileges to target the user for reasons unrelated to legitimate IT operations.
- Even if the user’s infraction was real, the admin’s actions breached professional trust and the code of ethics.

Consequences:

- Actions like unauthorized surveillance can create a hostile work environment, expose the organization to legal risk, and warrant termination.
- Such incidents highlight the necessity for ethical integrity, the proper use of authority, and the importance of due process.

Summary Table

Concept	Key Points
Authentication	Verification of user’s identity via one or more factors: something you know, have, or are.
Authentication Methods	SFA (one factor), MFA (two or more). MFA is best practice.
Proving Identity	Everyday use of multi-layered authentication (ATM, biometrics).
Risk in Our Lives	Daily risks (e.g. credit fraud), mitigated via MFA or insurance.
Code of Conduct	ISC2 requires highest ethical standards, defined in its Canons.
Ethical Examples	Unethical misuse of sensitive data, abuse of admin authority violates ethics code and can be more damaging than user infractions.

▼ Privacy Control Mechanisms

Concepts Covered:

- Privacy
- Privacy in the Working Environment
- What are Security Controls?
- Governance Elements
- Importance of Governance Elements

1. Privacy

Definition:

Privacy is the *right* of an individual to control the distribution and use of information about themselves.

Key Points:

- **Distinction from Security:** While both aim to safeguard personal and sensitive data, privacy specifically addresses *who* can access, share, or use the information, whereas security focuses on *protecting* data from risks such as breaches or unauthorized access.
- **Growing Significance:** As digital data collection increases across industries, so does the importance of privacy legislation and compliance.
- **Global Impact:** Privacy regulations affect organizations worldwide, often requiring compliance regardless of where a business is physically located.
- **Legal Frameworks:** Several ever-evolving laws define privacy and data protection, making awareness and adaptability essential for organizations.

Example: GDPR (General Data Protection Regulation)

- Passed by the European Union in 2016.
- Treats privacy as a fundamental human right.

- Applies to any organization handling data of individuals in the EU—regardless of where the company is based.
- US companies may also be governed by state privacy laws, which can differ in their scope and requirements.
- Noncompliance can lead to severe penalties or fines.

2. Privacy in the Working Environment

Context:

In the workplace, privacy is deeply intertwined with information security. Understanding the sensitivity of information helps determine suitable security controls.

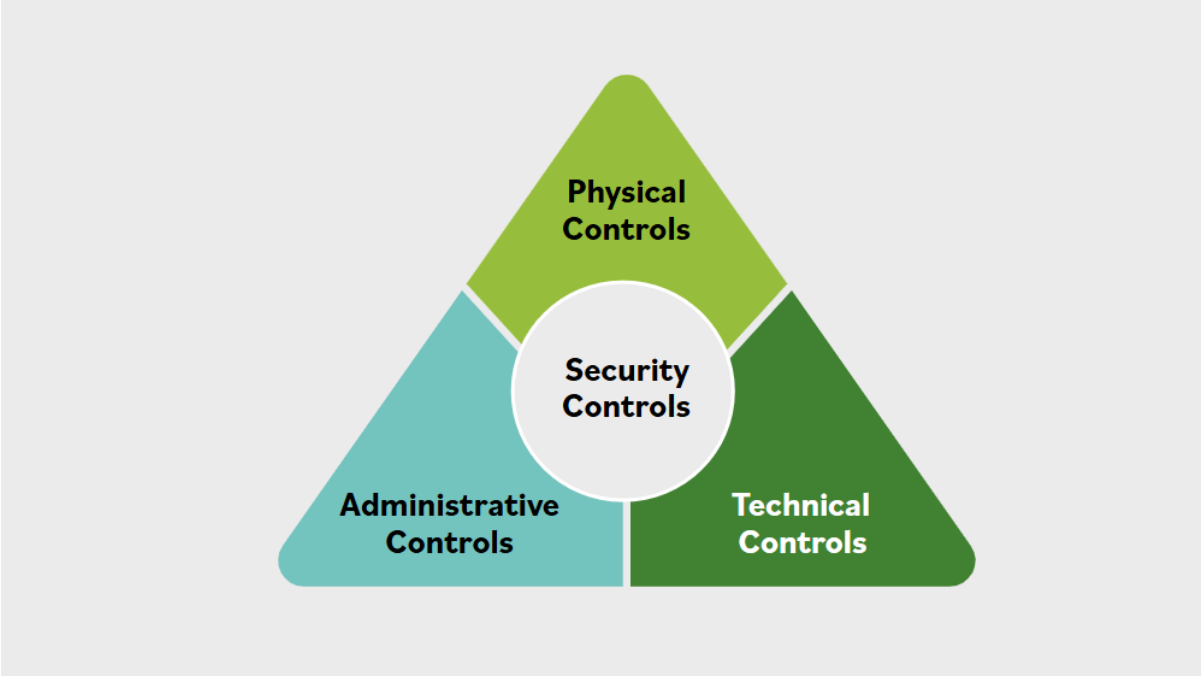
Key Points:

- **Regulations Vary by Region:**
  - *United States (US):* HIPAA (Health Insurance Portability and Accountability Act) governs medical data privacy.
  - *European Union (EU):* GDPR empowers individuals in the EU to control what personal information organizations can collect and store.
- **Global Operations:** Security professionals must be knowledgeable about the privacy laws in every jurisdiction where their company operates.
- **Compliance Abroad:** Organizations must respect and adapt to the privacy standards and legislation of each country in which they conduct business.

3. Security Controls

Overview:

Security controls are safeguards or countermeasures—physical, technical, and administrative—that protect the *confidentiality, integrity,* and *availability* of systems and data.



Types of Security Controls

A. Physical Controls

- Tangible mechanisms like badge readers, secure facility entry points, surveillance cameras, and physical barriers.
- Control and monitor the movement of people and equipment within controlled environments.
- Example: Employees using badges to access workplace entrances while visitors register at a central point.

B. Technical Controls (Logical Controls)

- Safeguards embedded in information systems and networks.
- Examples: Encryption, firewalls, access control lists, automated intrusion detection systems.
- Can include hardware and software settings or configurations.

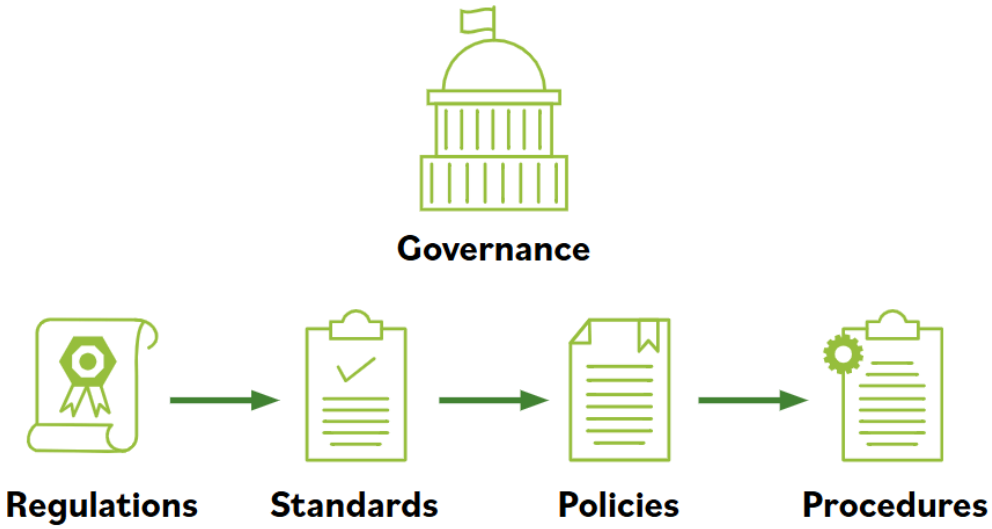
C. Administrative Controls (Managerial Controls)

- Policies, processes, directives, and guidelines affecting organizational behavior.
- Training, awareness campaigns, clear rules for data handling, and documented procedures.
- Effective when integrated into daily operational processes and decision making.

4. Governance Elements

Purpose:

Governance guides organizations in achieving their objectives through defined systems, structures, and processes backed by laws and standards.



The Hierarchy of Governance

1. **Regulations/Laws:**
    - Originating from governments, these are legal requirements that may include penalties for violations.
    - Examples:

    - *HIPAA (US, 1996):* Regulates the use and protection of personal health information (PHI).
    - *GDPR (EU):* Governs personal identifiable information (PII) within the EU and for EU citizens globally.
  - Organizations may be subject to overlapping regulations at national, regional, and municipal levels.
2. **Standards:**
  - Published frameworks providing best practices or mandatory requirements for industries.
  - Examples:
    - *ISO (International Organization for Standardization):* Offers global information security standards.
    - *NIST (National Institute of Standards and Technology, US):* Sets standards for IT and security, widely referenced internationally.
    - *IEEE (Institute of Electrical and Electronics Engineers):* Develops standards for telecommunications and computer engineering.
    - *IETF (Internet Engineering Task Force):* Creates networking and communication standards (e.g., internet protocols).
3. **Policies:**
  - High-level rules set by executive management informed by laws, standards, and organizational objectives.
  - Establishes priorities and the strategic direction, and provides a framework for compliance and decision-making.
  - Different organizational units (e.g., HR, finance, security) may have discrete policies aligned to overarching governance.
4. **Procedures:**
  - Step-by-step instructions for carrying out policies.
  - Specify how to perform tasks reliably and consistently.

- Include criteria for measuring effectiveness and training on proper execution.

Real-World Example:

Think of standards as the “grammar” for how computers communicate globally; through agreed-upon protocols and formats, systems interact seamlessly.

5. Importance of Governance Elements

Why It Matters:

- Regulations like *GDPR* and *HIPAA* significantly shape how organizations process and protect sensitive data, with strict compliance requirements and penalties for violations.
- Trust and credibility depend on robust information security. Breaches or mismanagement erode stakeholder confidence and can irreparably damage reputation.
- Compliance frameworks (e.g., from ISO) and detailed, regularly updated procedures are necessary to stay lawful and maintain high professional standards in safeguarding data.
- Proper governance ensures that all operational units work harmoniously towards compliance and security, reducing legal and reputational risks.

Additional Example:

- ISO standards may offer specific guidance, such as best practices for data destruction, thereby supporting legal compliance and strong organizational security.

By understanding privacy, security controls, and governance elements, organizations can better protect individual rights, manage risk, and ensure operational integrity in a rapidly evolving legal and technical landscape.

▼ Strategic Risk Management

Concepts Covered:

- Introduction to Risk Management
- Importance of Risk Management
- Risk Management Terminology
- Threats, Vulnerabilities, and Likelihood
- Risk Identification
- Risk Assessment
- Risk Treatment
- Risk Priorities
- Decision Making Based on Risk Priorities
- Risk Tolerance
- Risk Tolerance Drives Decision Making

---

1. Introduction to Risk Management

- **Definition & Role**:

  Risk management is a critical process within information assurance and cybersecurity that involves identifying, evaluating, and addressing risks that could affect an organization's operations and assets.

- **Objective**:

  Determine the acceptable level of risk and implement security controls to reduce risks to within that acceptable threshold.

- **Types of Risks**:
  - **Cyber risks**: cyber attacks including malware infections, social engineering scams, denial of service (DoS) attacks.
  - **Environmental risks**: physical threats like fire, violent crime, natural disasters (floods, earthquakes).
- **Process**:

- Identify vulnerabilities (weaknesses).
- Identify threats (potential harmful entities or events).
- Assess likelihood (probability) of occurrence.
- Determine potential impact on the organization.
- Deploy controls to mitigate identified risks.

2. Importance of Risk Management

- **Key Concepts**:
  - **Asset**: Anything valuable needing protection, e.g., information systems, facilities.
  - **Vulnerability**: Weakness or gap in defenses that exposes an asset.
  - **Threat**: Entity or event that can exploit a vulnerability to harm an asset.
- **Example**:

  A natural disaster like a major storm threatens the utility power supply, which is vulnerable to flooding. If power is cut off, IT systems will stop functioning, impacting operations.
- **Goal**:

  Evaluate the likelihood of risk events and take appropriate mitigating actions to protect valuable assets and ensure operations continue smoothly.

3. Risk Management Terminology

- **Asset**:

  Any resource or item of value that requires protection, such as data, hardware, personnel, or reputation.
- **Vulnerability**:

  A gap or weakness in protection that can be exploited.
- **Threat**:

A potential cause of unwanted incidents, which could exploit a vulnerability, resulting in harm.

- **Threat Actor**:

  Someone or something that carries out the threat, e.g., hackers, malware, natural events.

- **Threat Vector**:

  The method or path used by the threat actor to exploit the vulnerability.

4. Threats, Vulnerabilities, and Likelihood

- **Example Scenario**:

  Tourists in a crowded area are threatened by pickpockets (threat actors). The likelihood of being targeted depends on the tourist's vulnerability—such as being distracted, visibly carrying valuables, or appearing vulnerable.

- **Understanding**:

  Threats exist constantly, but whether a specific target is exploited depends on their vulnerability and attractiveness to the threat actor.

- **Threat Vector**:

  The particular approach taken by the threat actor, e.g., stealthily grabbing jewelry.

5. Risk Identification

- **What it is**:

  A continuous, ongoing process of recognizing possible risks within an environment.

- **How it works**:
  - Observe the environment for potential hazards (i.e., loose wires, water spills).
  - Analyze the organization's operations, processes, infrastructure, and personnel to uncover vulnerabilities and threats.

- **Who participates**:

  Everyone in the organization, at all levels, should be vigilant and report potential risks.

- **Role of Security Professionals**:

  Perform detailed system-level risk identification; assist or lead risk identification especially in organizations lacking formal risk management.

6. Risk Assessment

- **Definition**:

  The process of identifying, estimating, and prioritizing risks based on threat analysis, vulnerability analysis, and existing security controls.

- **Purpose**:
  - Determine which risks are most critical to the organization's mission, assets, and operations.
  - Align risks with organizational goals to guide decision-making.
- **Example**:

  Risk of fire to a building:

  - Fire alarms alert people and reduce injury risk but don't stop fire damage.
  - Sprinklers reduce fire spread but may damage equipment.
  - Gas-based suppression systems limit damage but may be costly.
- **Outcome**:

  A report or presentation aids management in prioritizing risk mitigation efforts or deciding on further in-depth assessments.

7. Risk Treatment (Risk Responses)

There are four primary ways to treat identified risks:

1. **Avoidance**:

Eliminating the risk entirely by stopping the risky activity.

Example: Canceling a project to avoid vulnerabilities exposure.

2. **Acceptance**:

   Choosing to accept the risk without action due to low impact or high cost of mitigation.

   Example: Accepting minor downtime risks to save on mitigation costs.

3. **Mitigation**:

   Implementing controls to reduce risk likelihood or impact.

   Example: Installing fire suppression, firewalls, or employee training.

4. **Transfer**:

   Shifting risk to another party, usually via insurance or outsourcing.

   Example: Cyber insurance covering data breach losses.

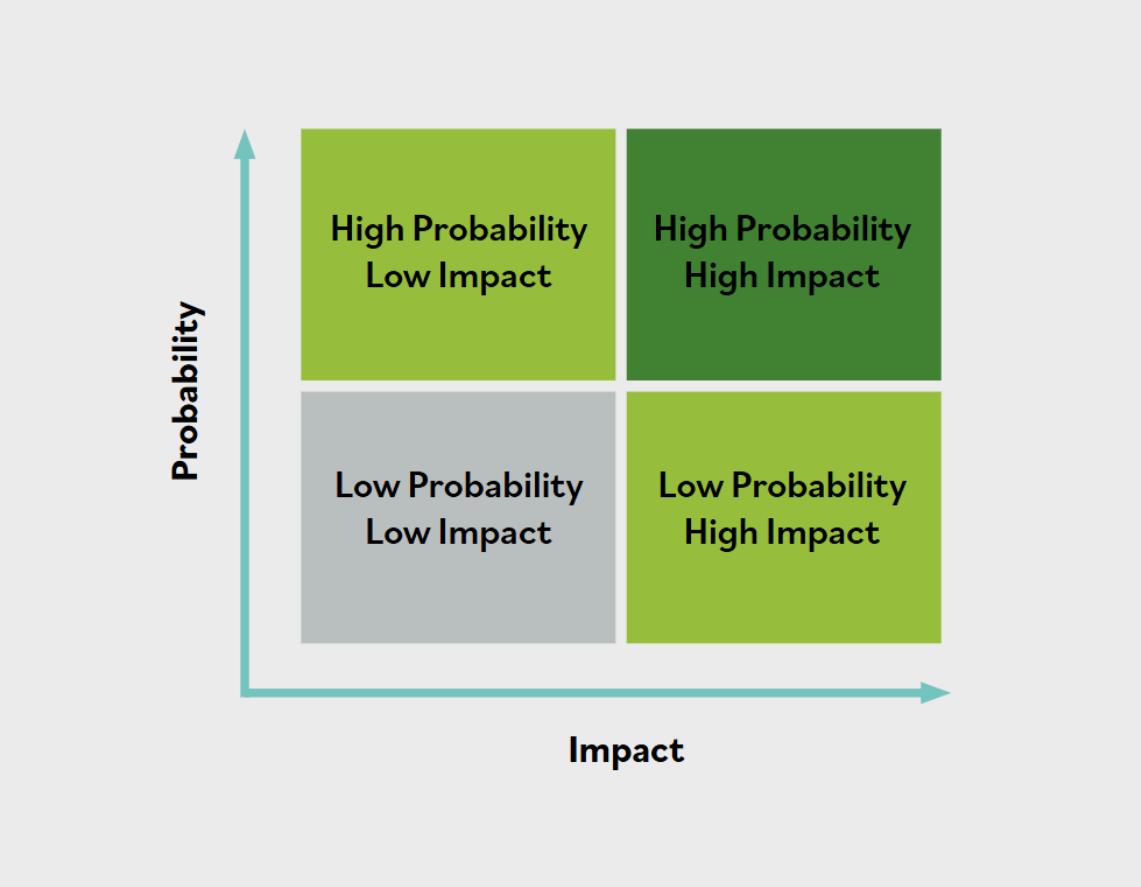
8. Risk Priorities

- **Why prioritize**:

  Effective risk management requires focusing resources on the most significant risks.

- **Methods**:
  - **Qualitative Analysis**: Assess risks based on expert judgment, categorizing risk severity (e.g., high, medium, low).
  - **Quantitative Analysis**: Use numerical data and statistical techniques to calculate probability and impact.

- **Risk Matrix**:



A tool plotting likelihood (probability) against impact to rank risks, introducing a common language for communicating risk status.

Quadrant	Description	Example in Cybersecurity
High Probability, Low Impact	These risks happen often but rarely cause serious harm.	Frequent phishing attempts blocked by spam filters.
High Probability, High Impact	The most dangerous: happen often and can cause significant damage.	Ongoing ransomware threats in an under-secured organization.
Low Probability, Low Impact	Minor concerns: rare and not harmful when they do occur.	Occasional failed login attempts with no access gained.
Low Probability, High Impact	Rare, but very significant if they happen.	Major data breach from exploiting an unknown vulnerability.

- **Impact**:

Can be financial, operational, reputational, or safety-related.

9. Decision Making Based on Risk Priorities

- **Decision factors**:
  - Likelihood and impact of risks.
  - Organization's risk tolerance (how much risk is acceptable).
  - Geographic or contextual factors influencing risk exposure.
- **Example**:
  - Companies in Hawaii prioritize volcanic eruption risks, while Chicago-based companies focus more on blizzards.
  - Ignoring known risks (like asbestos exposure) can create severe liability.

10. Risk Tolerance

- **Definition**:

  The degree to which an organization (usually determined by executive management/board) is willing to accept risk.
- **Factors influencing tolerance**:
  - Organizational culture and attitude toward risk.
  - Location and exposure to natural or man-made hazards.
  - Financial standing, business models, and operational priorities.
- **Variations within an organization**:

  Different departments may vary in risk acceptance depending on their function.
- **Example**:
  - Iceland companies accept volcanic risks and plan accordingly.
  - Organizations in areas prone to frequent power outages may invest heavily in backup power systems proportional to their tolerance for

downtime.

11. Risk Tolerance Drives Decision Making

- **Examples**:
  - **Business bid**: An organization invests $10,000 in a proposal to win a potential $2 million contract — accepting financial risk because of the rewarding opportunity (risk within tolerance).
  - **Trauma center**: Zero tolerance for power failure leads to multiple power redundancy measures to ensure uninterrupted patient care.
  - **Entrepreneurs**: Liza and Chris accept risk of business failure based on the perceived high reward of starting their venture.
- **Conclusion**:

  Decisions on risk management are ultimately driven by the organization's appetite for risk balanced against potential rewards.