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

The **CIA Triad** is a foundational model in information security, representing three core principles:

- **Confidentiality**
- **Integrity**
- **Availability**

These principles help organizations define, understand, and manage security in a way that is meaningful to both technical and non-technical stakeholders.

1. Confidentiality

Definition

- **Confidentiality** means allowing only authorized individuals to access information, while protecting it from unauthorized disclosure.

Key Concepts

- **Authorized Access:** Only users with proper permissions can view or use certain information.

- **Protection from Disclosure:** Preventing sensitive data from being exposed to outsiders.

Examples

- **Banking:** Customer account details are accessible only by the account holder and authorized bank staff.
- **Healthcare:** Medical records are restricted to patients and healthcare providers.

Related Terms

- **Personally Identifiable Information (PII):** Data that can identify an individual (e.g., name + date of birth).
- **Protected Health Information (PHI):** Health-related data tied to an individual.
- **Classified/Sensitive Information:** Trade secrets, business plans, or intellectual property.
- **Sensitivity:** The importance or criticality assigned to information, dictating how it should be protected.

Challenges

- Balancing access for legitimate users (including guests or customers) with the need to protect data from unauthorized access.
- Ensuring data remains confidential even when accessed through potentially compromised devices or applications.

2. Integrity

Definition

- **Integrity** ensures that information is complete, accurate, consistent, and reliable for its intended purpose.

Key Concepts

- **Data Integrity:** Data must not be altered without authorization; it should be free from errors and unauthorized changes.
- **System Integrity:** Systems must operate as intended and maintain a known, good configuration.
- **Internal Consistency:** Information should be the same across all systems and instances.

Examples

- **Medical Records:** If unauthorized changes are made to a patient's medical history, it could endanger their health.
- **Financial Systems:** Unauthorized modification of transaction records could lead to financial loss or fraud.

How Integrity is Maintained

- **Baselines:** Establishing a known good state of data or systems for comparison.
- **Monitoring:** Regularly checking current state against the baseline to detect unauthorized changes.
- **Legal/Regulatory Requirements:** Laws may require certain information to remain unaltered and accurate.

3. Availability

Definition

- **Availability** means that systems and data are accessible to authorized users when needed, in the required form and format.

Key Concepts

- **Timely Access:** Information must be available when users need it.
- **Reliability:** Systems should function as required to support business operations.

- **Criticality:** Some systems/data are more vital than others; their availability must be prioritized.

Examples

- **Ransomware Attack:** Attackers lock access to data, disrupting business until a ransom is paid.
- **Power Outage:** If backup generators fail, systems may become unavailable.

Maintaining Availability

- **Redundancy:** Backup systems and data copies.
- **Disaster Recovery Plans:** Procedures to restore access after disruptions.
- **Identifying Critical Systems:** Prioritize resources to ensure essential services remain available.

Real-World Application of the CIA Triad

- **Confidentiality:** Protecting PII in banking, healthcare, and insurance.
- **Integrity:** Preventing unauthorized changes to critical information (e.g., medical or financial data).
- **Availability:** Ensuring employees and customers can access information and services when needed; mitigating risks from cyberattacks like ransomware.

Non-Repudiation

Definition

- **Non-repudiation** ensures that individuals cannot deny their actions (such as creating, approving, sending, or receiving information).

Importance

- **Legal Accountability:** Holds individuals responsible for their actions, preventing denial of transactions or communications.

- **E-commerce:** Prevents users from denying online purchases or actions.
- **Technical Methods:** Digital signatures, audit logs, and receipts are used to provide proof of actions.

Protecting Information

- **PII Protection:** A single data point (like a date of birth) may not be sensitive, but when combined with other data (like a name), it can become PII and must be protected.
- **Everyday Relevance:** The CIA triad is present in daily activities—when visiting a doctor, checking email, or accessing bank accounts, professionals are entrusted to maintain these security principles.

Threats to the CIA Triad

Human Factors

- **Password Sharing:** If employees share passwords, unauthorized access can occur even after someone leaves the organization.
- **Malicious Insiders:** Disgruntled former employees may use retained credentials to harm systems or data.

Technical Factors

- **Malware:** Unauthorized software can compromise data integrity or confidentiality.
- **Unattended Devices:** Family members using a work laptop can inadvertently introduce threats.

Environmental Factors

- **Power Outages:** Backup systems may fail if not properly maintained, affecting availability.
- **Fire Suppression:** Inadequate methods can destroy both digital and paper records, impacting all three CIA elements.

Risk Management

- **Comprehensive Risk Assessment:** Identify technical, human, and environmental threats.
- **Mitigation Strategies:** Implement controls and procedures to protect information and maintain the CIA triad.

Summary Table: CIA Triad Concepts

Principle	Definition	Example Scenario	Threats/Challenges
Confidentiality	Only authorized access; prevent improper disclosure	Protecting patient records in hospitals	Data leaks, unauthorized access
Integrity	Completeness, accuracy, consistency, and reliability of information	Preventing unauthorized changes to financial records	Data corruption, insider threats
Availability	Reliable, timely access for authorized users	Ensuring online banking services are accessible during business hours	System failures, DoS attacks, disasters
Non-repudiation	Preventing denial of actions; ensuring accountability	Digital signatures on contracts	Lack of audit trails, weak authentication

▼ 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 the identity of a user or system after they claim an identity. It ensures that the person or system requesting access is legitimate.

Three Common Methods of Authentication:

- **Something You Know:**

  Passwords, passphrases, or PINs that only the user should know.

  Example: Entering a password to log into an email account.

- **Something You Have:**

  Physical items like tokens, smart cards, or memory cards that the user possesses.

  Example: Using a security token to access a corporate network.

- **Something You Are:**

  Biometrics such as fingerprints, facial recognition, or iris scans.

  Example: Unlocking a smartphone using fingerprint recognition.

2. Methods of Authentication

Single-Factor Authentication (SFA)

- Uses only one of the authentication methods (knowledge, possession, or biometrics).
- *Example:* Logging in with just a password.
- **Limitation:** Vulnerable if that single factor is compromised.

Multi-Factor Authentication (MFA)

- Requires two or more different authentication factors.
- *Example:* Using a password plus a code sent to your phone.
- **Benefit:** Provides stronger security by reducing the risk of unauthorized access.

Best Practice:

Implement at least two of the three common authentication techniques (knowledge-based, token-based, characteristic-based) for better security.

3. Knowledge-Based Authentication

- Relies on secrets like passwords or PINs.
- Vulnerable to social engineering, phishing, or unauthorized password resets.
- *Example:* A help desk resetting a password for someone pretending to be the user.
- **Mitigation:** Combine with token-based or biometric authentication to enhance security.

Note: Using both a username and password counts as two things known but is still single-factor authentication because both are from the same category.

4. Proving Identity in Daily Life

- Commonly involves multiple factors without users realizing it.
- *Example:* Using an ATM card (something you have) and a PIN (something you know) is MFA.
- Biometrics add another layer of security, such as fingerprint or facial recognition on phones.

5. Risk in Our Lives

- **Example:** Unauthorized credit card charges can cause inconvenience and require card replacement.

- **Mitigation:** Avoid storing credit card info on devices, use MFA for banking accounts.
- Insurance (travel, health, identity theft) is a way to transfer or mitigate risk.
- Companies offering identity theft protection manage financial risk by balancing premiums and payouts.

6. Professional Code of Conduct

ISC2 Code of Ethics Preamble

The Preamble states the purpose and intent of the ISC2 Code of Ethics.

- The safety and welfare of society and the common good, duty to our principles, and duty to each other require that we adhere and be seen to adhere to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

ISC2 Code of Ethics Canons

The Canons represent the important beliefs held in common by the members of ISC2. Cybersecurity professionals who are members of ISC2 have a duty to the following four entities in the Canons.

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principles.
- Advance and protect the profession

7. Theoretical Examples: Code of Ethics

Example 1: Misuse of Biometric Data

- An organization uses retinal scans to discriminate against female candidates (detecting pregnancy).

- This violates ethical principles requiring honesty, justice, and legal behavior.

Example 2: Abuse of Authority in Monitoring

- A network administrator monitors a user without proper authority due to personal conflict.
- Although the user violated policy, the administrator's misuse of power is a more serious ethical breach.
- This behavior risks legal consequences and damages workplace trust.

Summary Table

Concept	Explanation & Example
Authentication	Verifying identity using knowledge, possession, or biometrics.
Single-Factor Authentication	One method only (e.g., password). Less secure.
Multi-Factor Authentication	Two or more methods (e.g., password + token). More secure.
Knowledge-Based Authentication	Something you know (password). Vulnerable alone.
Token-Based Authentication	Something you have (card, token).
Biometric Authentication	Something you are (fingerprint, face).
Risk Management	Identify risks and mitigate with controls like MFA or insurance.
ISC2 Code of Ethics	Security professionals must act ethically and protect society.
Ethical Dilemmas	Misuse of sensitive data or authority violates ethics and can cause legal issues.

▼ 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 how information about themselves is distributed.
- **Privacy vs. Security:**
  - *Privacy* is about controlling access to personal information.
  - *Security* is about protecting data from unauthorized access, but does not guarantee privacy.
  - **Example:** A company may have strong security (e.g., encrypted databases) but still violate privacy by sharing user data without consent.
- **Legislation and Compliance:**
  - Due to growing data collection and digital storage, privacy laws and compliance requirements are increasing globally.
  - Laws may change frequently, requiring organizations to stay updated.
  - **Example:** The European Union's General Data Protection Regulation (GDPR) treats privacy as a fundamental human right and applies to any organization handling EU residents' data, regardless of the company's location.
- **Global Impact:**
  - Privacy regulations can affect organizations worldwide, not just those physically located in a specific country.

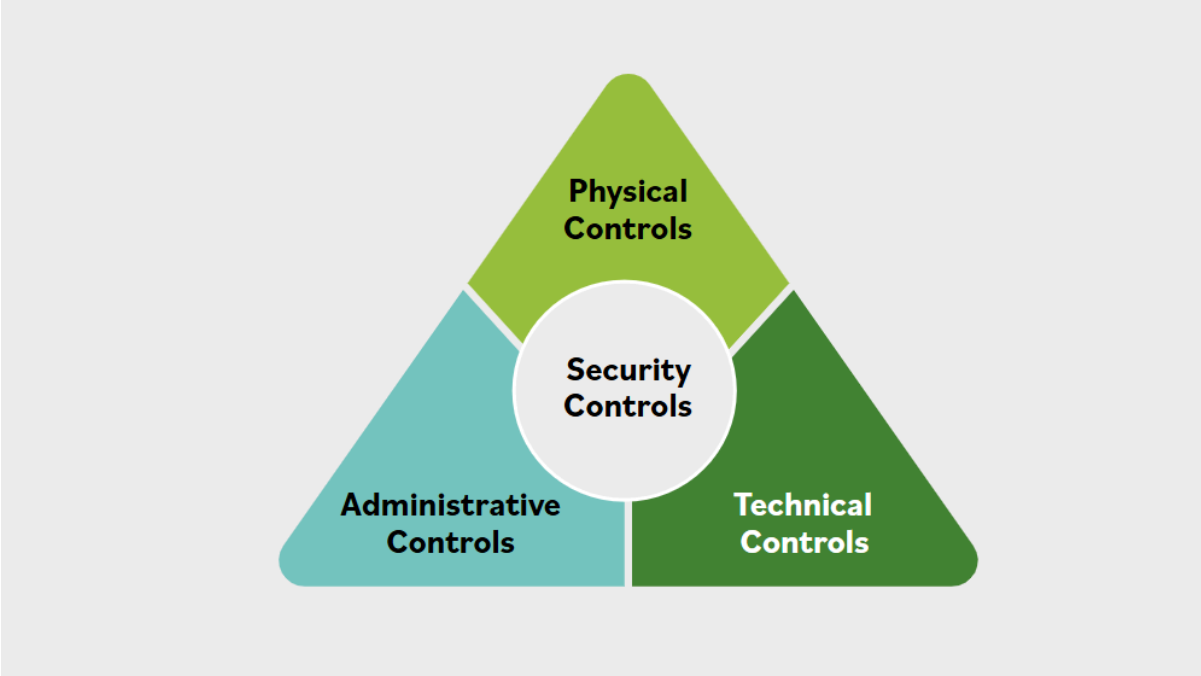
- **Example:** A U.S. company serving EU customers must comply with GDPR.

2. Privacy in the Working Environment

- **Role in Information Security:**
  - Privacy is a key part of information security. Knowing the sensitivity of information helps determine the necessary controls.
- **Standards, Policies, and Procedures:**
  - Privacy requirements in the workplace are governed by various standards and laws, which differ by region.
  - **Examples:**
    - *HIPAA (U.S.):* Regulates privacy of medical information.
    - *GDPR (EU):* Gives individuals control over their data.
- **Compliance Awareness:**
  - Security professionals must be aware of privacy laws in all regions where their organization operates.
  - When operating internationally, organizations must follow the most stringent applicable privacy standards.

3. Security Controls

Security controls are measures used to safeguard the confidentiality, integrity, and availability of information systems.



a. Physical Controls

- **Definition:** Physical safeguards using hardware or physical barriers.
- **Examples:**
  - Badge readers, security doors, fences, surveillance cameras.
  - Controlled entry points for visitors and employees.
- **Integration:** Often combined with technical controls (e.g., badge readers connected to access control systems).

b. Technical Controls (Logical Controls)

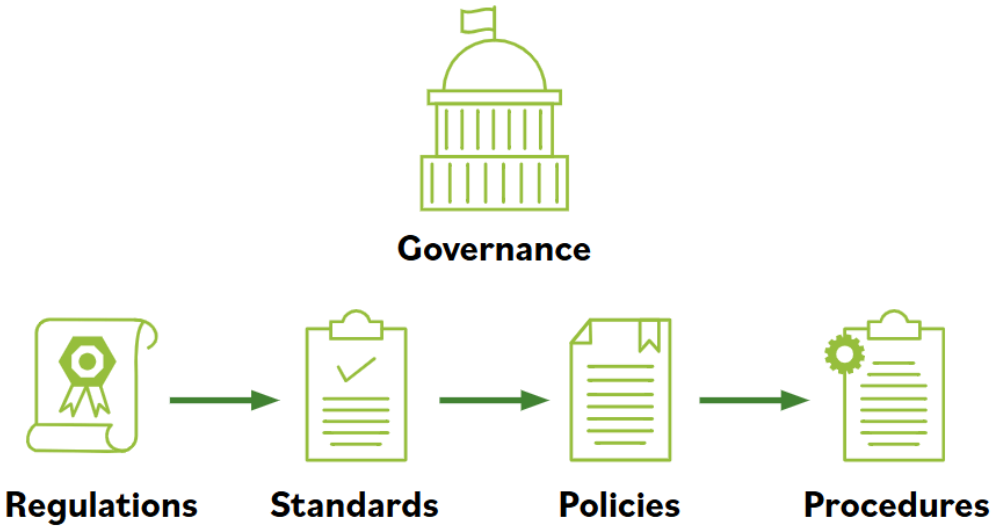
- **Definition:** Automated controls implemented by computer systems and networks.
- **Examples:**
  - Firewalls, encryption, access control lists, intrusion detection systems.
  - Software settings (e.g., password policies), hardware configurations.
- **Considerations:** Require careful management and operational oversight to align with organizational security policies.

c. Administrative Controls (Managerial Controls)

- **Definition:** Policies, procedures, and guidelines that direct human behavior.
- **Examples:**
  - Security awareness training, incident response plans, hiring practices.
  - Written policies that set expectations for staff.
- **Implementation:** Should be integrated into daily operations, not just reserved for senior management decisions.

4. Governance Elements

Governance ensures organizations achieve their objectives while complying with laws and regulations.



a. Hierarchy of Governance Elements

Element	Description & Example
Regulations	Laws issued by governments (e.g., HIPAA, GDPR); carry penalties for non-compliance.
Standards	Frameworks created to support regulations (e.g., ISO, NIST standards).

Element	Description & Example
Policies	Organization-specific rules informed by laws and standards (e.g., data retention policy).
Procedures	Step-by-step instructions for tasks (e.g., how to securely destroy data).

b. Regulations and Laws

- **Enforcement:** Can be imposed at national, regional, or local levels.
- **Examples:**
  - *HIPAA (U.S.):* Governs health information; violations can lead to fines or imprisonment.
  - *GDPR (EU):* Controls personal data use; applies globally to entities handling EU residents' data.
- **Multi-level Compliance:** Organizations may be subject to multiple overlapping regulations and must comply with the most restrictive.

c. Standards

- **Purpose:** Provide assurance that organizations follow best practices and comply with regulations.
- **Major Standards Bodies:**
  - *ISO (International Organization for Standardization):* Publishes global standards, including for information security.
  - *NIST (National Institute of Standards and Technology):* U.S. agency that sets standards, widely adopted globally.
  - *IETF (Internet Engineering Task Force):* Sets standards for internet protocols, enabling global computer communication.
  - *IEEE (Institute of Electrical and Electronics Engineers):* Develops standards for telecommunications and computing.

d. Policies

- **Nature:** Broad, high-level statements that set strategic direction and priorities.
- **Levels:** Can exist at various organizational levels (executive, departmental, functional).
- **Implementation:** Policies must be translated into actionable procedures for effective compliance.

e. Procedures

- **Definition:** Detailed, repeatable steps for accomplishing specific tasks.
- **Purpose:** Ensure consistency, provide decision criteria, and define success metrics.
- **Importance:** Proper documentation and training are essential for effective use.

5. Importance of Governance Elements

- **Operational Impact:** Regulations and laws directly influence daily operations, especially in data-sensitive industries.
- **Trust and Credibility:** Effective information security builds trust; breaches can irreparably damage reputation.
- **Compliance Frameworks:** Published standards (e.g., ISO on secure data destruction) guide organizations in developing compliant policies and procedures.
- **Continuous Improvement:** Organizations must regularly review and update their policies, standards, and procedures to remain compliant and effective.

Summary Table: Key Concepts and Examples

Concept	Description	Example
Privacy	Control over personal data	GDPR, HIPAA
Physical Control	Hardware-based security	Badge readers, security doors
Technical Control	Automated system safeguards	Firewalls, encryption

Concept	Description	Example
Administrative Control	Policies and training for people	Security awareness programs
Regulation	Government-imposed law	HIPAA, GDPR
Standard	Industry best practice framework	ISO 27001, NIST SP 800-53
Policy	Organization's rules for compliance	Data retention policy
Procedure	Step-by-step task instructions	Secure data destruction process

▼ 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

Introduction to Risk Management

- **Risk Management in Cybersecurity:**

- Central to information assurance and cybersecurity.
- The level of cybersecurity needed depends on the level of risk an organization is willing to accept.
- **Risk**: The potential consequences of events in the environment (e.g., cyberattacks, natural disasters).
- **Security Controls**: Measures implemented to reduce risk to acceptable levels.
- **Examples**:
  - Cyber risks: Malware, social engineering, denial of service (DoS) attacks.
  - Non-cyber risks: Fire, violent crime, natural disasters.
- **Risk Management Technologies**: Help identify vulnerabilities and threats, and assess their likelihood and impact.

Importance of Risk Management

- **Vulnerability**:
  - A weakness or gap in protection of valuable assets (e.g., outdated software, unlocked doors).
- **Threat**:
  - Anything or anyone that can exploit a vulnerability to cause harm (e.g., hackers, storms).
- **Example**:
  - A storm (threat) causes flooding (exploits vulnerability in power supply), making IT systems (asset) unavailable.
- **Risk Evaluation**:
  - Assess the likelihood of events and take actions to mitigate them.

Risk Management Terminology

- **Asset**:

    - Anything valuable that needs protection (e.g., data, hardware, people).
- **Vulnerability**:
    - Weaknesses in protection efforts (e.g., unpatched software, weak passwords).
- **Threat**:
    - Entity or event that exploits a vulnerability (e.g., cybercriminals, natural disasters).

Threats, Vulnerabilities, and Likelihood

- **Example: Pickpockets and Tourists**
    - **Threat**: Pickpockets in a crowded area.
    - **Vulnerability**: Tourists who are distracted or have valuables exposed.
    - **Threat Actor**: The pickpocket.
    - **Threat Vector**: The technique used (e.g., distraction, snatching).
    - **Likelihood**: Increases if the target appears more vulnerable.

Risk Identification

- **Ongoing Process**:
    - Not a one-time activity; must be repeated as new risks emerge.
- **Involves**:
    - Identifying, characterizing, and estimating potential disruptions.
- **Responsibility**:
    - All employees, not just security professionals, should identify risks.
- **Example**:
    - Noticing loose wires (physical risk) or outdated software (cyber risk).
- **Security Professionals' Role**:

- Assist in risk assessment, process control, monitoring, incident response, and recovery.

Risk Assessment

- **Definition**:
  - Identifying, estimating, and prioritizing risks to operations, assets, individuals, and reputation.
- **Process**:
  - Analyze threats and vulnerabilities, consider existing controls.
  - Align risks with organizational goals and objectives.
- **Example**:
  - Fire risk in a building:
    - **Mitigations**: Fire alarms (alert), sprinklers (limit damage), gas-based systems (protect equipment).
    - **Prioritization**: Management decides which control is best based on cost and effectiveness.
- **Output**:
  - Documented report for management to review and approve.
  - May lead to more in-depth assessments if needed.

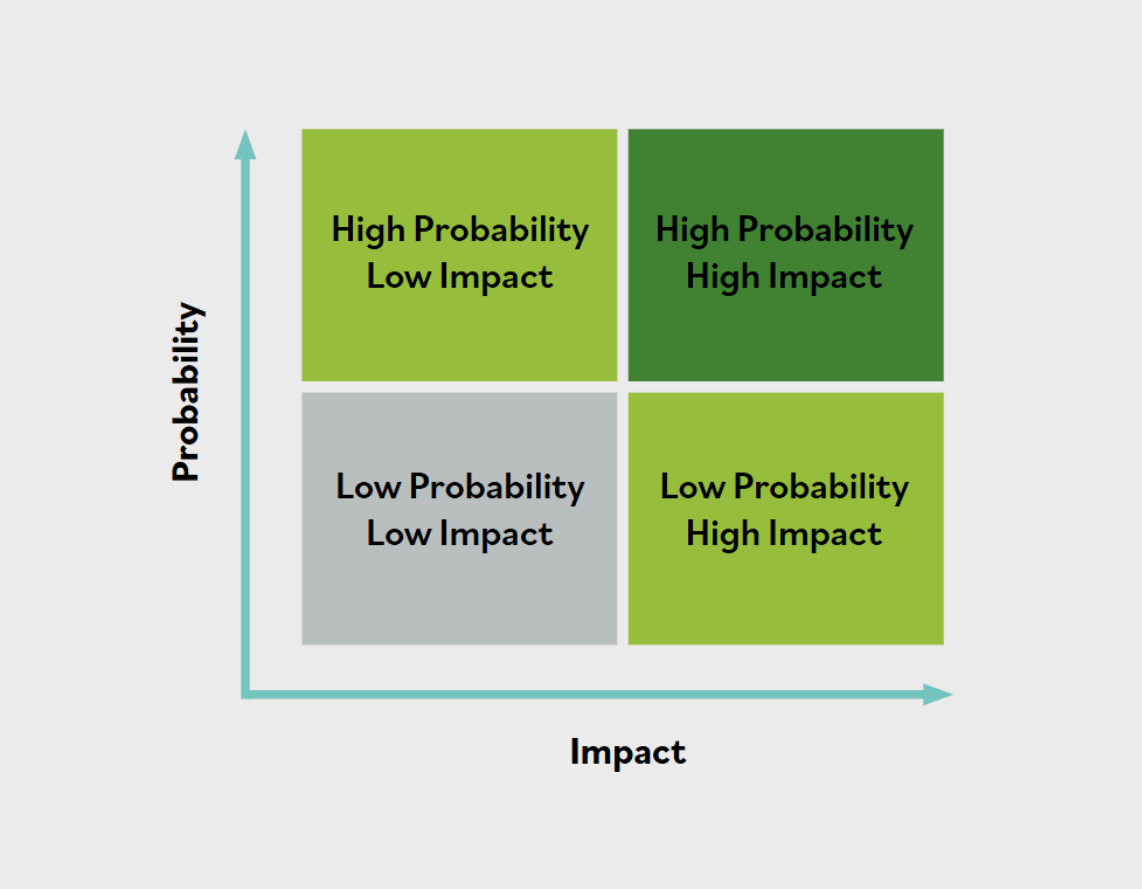
Risk Treatment

- **Making Decisions**:
  - Decide how to handle each risk based on management's attitude and available resources.
- **Options**:
  1. **Avoidance**:
     - Eliminate the risk (e.g., stop risky activities).
     - Example: Discontinue a service that is too risky.

2. **Acceptance**:
    - Do nothing; accept the risk if impact is low or benefits outweigh risks.
    - Example: Continue a low-risk operation without extra controls.
3. **Mitigation**:
    - Reduce the risk via controls, policies, procedures.
    - Example: Install antivirus software, train employees.
4. **Transfer**:
    - Pass risk to another party (usually through insurance).
    - Example: Buy cyber insurance to cover financial loss from data breaches.

Risk Priorities

- **Prioritization**:
    - Analyze and rank risks using qualitative (descriptive) or quantitative (numerical) methods.
    - **Qualitative Risk Analysis:** A subjective assessment of risk, often using descriptive terms (e.g., high, medium, low) to evaluate likelihood and impact. It's useful for quickly prioritizing risks and understanding their relative importance without precise numerical data.
    - **Quantitative Risk Analysis:** An objective, numerical assessment of risk, assigning specific monetary values or probabilities to the likelihood and impact of risks. This method provides a more detailed cost-benefit analysis and aids in making financially informed decisions.
- **Risk Matrix**:
    - Tool that plots likelihood vs. impact to assign priority.
    - Example:
        - Low likelihood + low impact = low priority.
        - High likelihood + high impact = high priority.



- **Business Context**:
  - Priorities may depend on cost, business objectives, or potential loss.

Decision Making Based on Risk Priorities

- **Evaluate**:
  - Likelihood, impact, and organizational risk tolerance.
- **Example**:
  - Hawaii company plans for volcanic eruptions, Chicago company for blizzards.
- **Management's Role**:
  - Decide what risks to accept, mitigate, or avoid based on tolerance and liability.

Risk Tolerance

- **Definition**:
  - The amount of risk an organization is willing to accept.
- **Varies**:
  - Between organizations and even departments.
- **Determined By**:
  - Executive management or Board of Directors.
- **Geographic Example**:
  - Icelandic companies plan for volcanoes; others may not.
- **Downtime Example**:
  - Frequent power outages → invest in generators.
  - Critical operations (e.g., hospitals) → multiple backup systems.

Risk Tolerance Drives Decision Making

- **Examples**:
  1. **Business Bid**:
     - Cost to build bid ($10,000), potential contract ($2 million).
     - Organization accepts risk of losing bid due to high reward.
  2. **Trauma Center**:
     - Zero tolerance for power failure.
     - Multiple redundancies: utility providers, batteries, generators, fuel contracts.
  3. **Entrepreneurship**:
     - Liza and Chris quit jobs to start a business, accepting risk of failure for potential reward.

Summary Table

Step	Key Points
Risk Identification	Ongoing process, all employees involved, focus on unique org. situation
Risk Assessment	Analyze threats/vulnerabilities, align with org. goals, prioritize risks
Risk Treatment	Avoid, accept, mitigate, or transfer risks based on management attitude and resources
Risk Prioritization	Use risk matrix, qualitative/quantitative analysis, align with business priorities
Decision Making	Based on risk priorities and tolerance, management sets acceptable risk levels
Risk Tolerance	Varies by org., context, and department; drives investment and operational decisions