

Introduction to Mitigation Techniques

Introduction to Mitigation Techniques

Focus: Core concepts, categories, and practical steps for reducing risk in information security, project management, and environmental contexts.

1. What Is Mitigation?

Aspect	Definition
General	The process of reducing the severity, impact, or likelihood of an unwanted event.
Security	Controls and actions taken to limit the damage caused by threats or vulnerabilities.
Project Management	Strategies to lower the probability or impact of risks that could derail a project.
Environmental	Measures that lessen the negative effects of human activities on ecosystems.

Key Idea: Mitigation ≠ elimination. It aims to *manage* risk to an acceptable level when total removal is impractical or too costly.

2. Mitigation Lifecycle Framework

1. **Identify** – Recognize potential threats, hazards, or risks.
2. **Assess** – Evaluate likelihood and potential impact (quantitative or qualitative).
3. **Prioritize** – Rank based on risk score or business impact.
4. **Select Controls** – Choose appropriate mitigation techniques.
5. **Implement** – Deploy controls, assign responsibilities, allocate resources.
6. **Monitor & Review** – Track effectiveness, adjust as conditions change.

(The loop repeats continuously; mitigation is an ongoing activity.)

3. Major Categories of Mitigation Techniques

Introduction to Mitigation Techniques

Category	Typical Use Cases	Representative Techniques
Technical / Engineering	Cybersecurity, system reliability, product design	• Firewalls, IDS/IPS • Patch management • Redundant architectures (RAID, clustering) • Input validation, encryption
Administrative / Procedural	Organizational risk, compliance	• Policies & standards • Training & awareness programs • Incident response playbooks • Access control reviews
Physical / Environmental	Facility protection, environmental stewardship	• Surveillance cameras, security guards • Fire suppression systems • Flood barriers, seismic bracing • Waste reduction programs
Financial / Insurance	Business continuity, project budgeting	• Risk transfer via insurance • Contingency reserves • Hedging contracts
Legal / Regulatory	Governance, liability management	• Contractual clauses (indemnities, SLAs) • Compliance audits, certifications (ISO 27001, PCI-DSS)
Strategic / Organizational	Long-term resilience, market positioning	• Diversification of suppliers • Business continuity planning (BCP) • Scenario planning and tabletop exercises

4. Common Mitigation Techniques (Examples)

4.1. Defense in Depth (Layered Security)

- **Goal:** Multiple, independent controls so that failure of one does not expose the asset.
- **Layers:** Perimeter ? Network ? Host ? Application ? Data ? User.

Introduction to Mitigation Techniques

- **Typical controls:** Firewalls ? IDS/IPS ? Host?based antivirus ? Secure coding ? Encryption ? MFA.

4.2. Least Privilege & Role?Based Access Control (RBAC)

- **Goal:** Users receive only the permissions needed for their role.
- **Implementation steps:**
 1. Define roles and required permissions.
 2. Map users to roles.
 3. Enforce via directory services (Active Directory, LDAP).
 4. Review periodically (e.g., quarterly).

4.3. Patch Management

- **Goal:** Close known software vulnerabilities before they can be exploited.
- **Process:**
 1. Inventory assets.