Information Security Principles

Information Security Principles

- Confidentiality
- Integrity
- Availability

Information Security Principles

- Authenticity
- Non-Repudiation
- Accountability

Information Security Governance

Information Security Governance

- Establishing organizational policies, roles, and responsibilities
- Defining the information security framework (e.g., ISO 27001, NIST)
- Implementing a risk management program
- Ensuring compliance with legal and regulatory requirements

Risk Management and Compliance

Identifying Risks

Identifying Risks

- Threat assessment
- Vulnerability analysis
- Impact assessment

B. Evaluating Risks

Evaluating Risks

- Quantitative methods (e.g., OCTAVE, FAIR)
- Qualitative methods (e.g., Risk Matrix, Heat Map)

Mitigating Risks

Mitigating Risks

- Implementing security controls
- Reducing vulnerabilities
- Transferring risk through insurance or contracts

Protecting and Defending Assets

Physical Security

Physical Security

- Access control
- Environmental protection
- Incident response planning

Network Security

Network Security

- Firewalls, intrusion detection systems (IDS), antivirus software
- Virtual Private Networks (VPN)
- Encryption

Application Security

Application Security

- Code reviews
- Input validation and output encoding
- Access control and authentication

Security Management Plans

Security Management Plans

- Developing a security plan to address organizational risks
- Allocating resources and responsibilities for its implementation
- Regularly reviewing, testing, and updating the plan

Managing Incidents and Operations

Preparation

Preparation

- Defining incident response roles and responsibilities
- Developing an incident management policy

Detection and Analysis

Detection and Analysis

- Monitoring systems for signs of attacks
- Analyzing threats, vulnerabilities, and risks

Containment, Eradication, and Recovery

Containment, Eradication, and Recovery

- Limiting the impact of incidents
- Eliminating the root cause of attacks
- Restoring affected systems and data

Reporting and Lessons Learned

Reporting and Lessons Learned

- Documenting incident details for future analysis
- Sharing knowledge with teams, stakeholders, and the organization to improve security practices