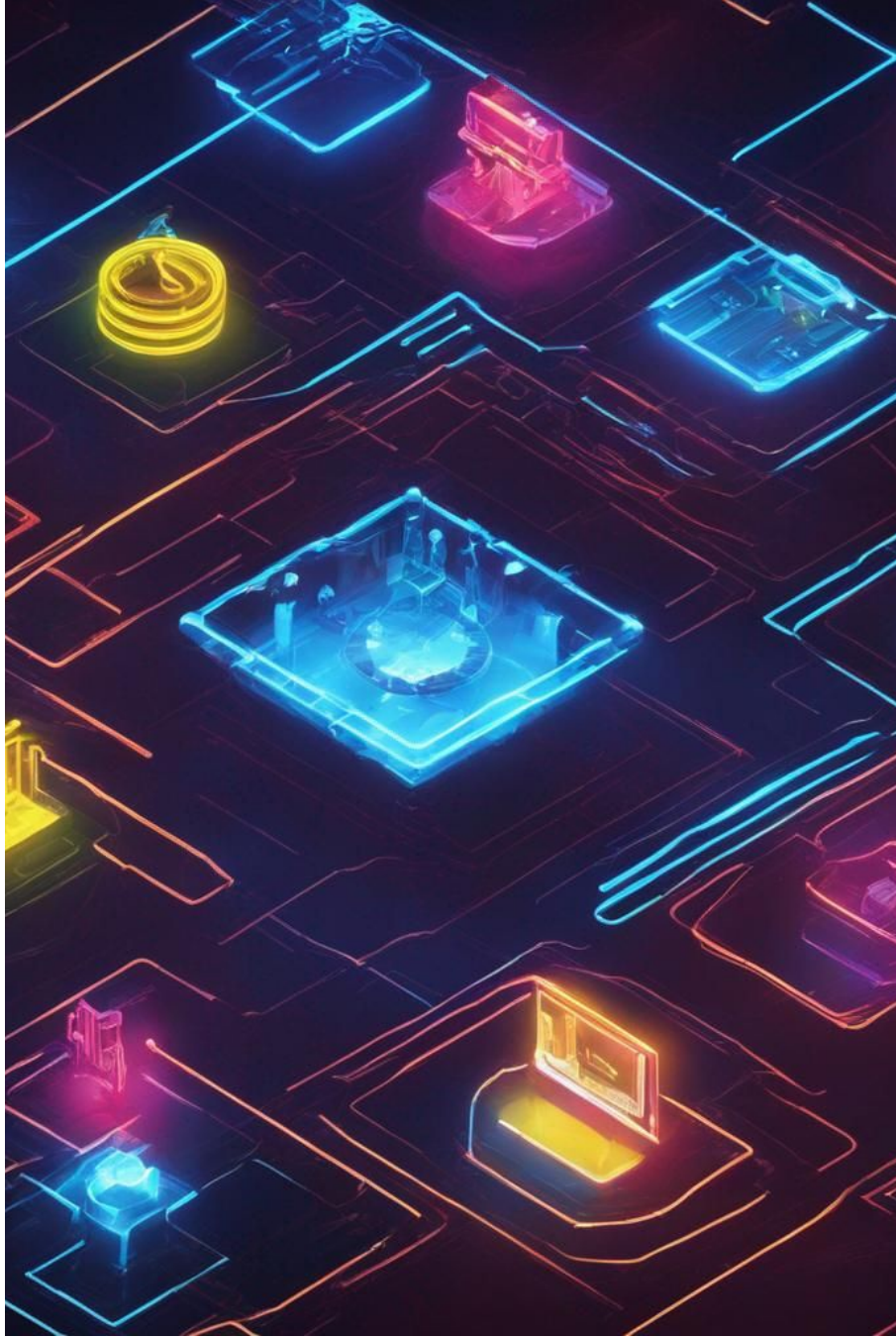
Securing the Future

Navigating Information Security Governance, Risk Management, and Frameworks

CISSP Study Guide - VI



Introduction to Information Security Governance and Risk Management

- **Overview:** Understanding how to protect data and manage risks

> **Confidentiality:** Data protection from unauthorized access
>
> **Integrity:** Ensuring data accuracy and reliability
>
> **Availability:** Data is accessible and usable when required

Identifying the Weaknesses

1. **Vulnerability:** Weak points in security measures

2. **Threat:** Potential for exploitation of vulnerabilities

3. **Threat Agents:** Entities potentially exploiting vulnerabilities

Understanding Risk in Security

Risk: Potential for threat agents to cause harm

Exposure: The extent of potential losses

Countermeasures: Controls to reduce risks

Due Diligence & Care: Steps taken to protect and to mitigate damages

Personnel Security Practices

- **Job Rotation:** Prevents fraud and increases redundancy
- **Separation of Duties:** Limits power of individuals
- **Split Knowledge and Dual Control:** Ensures tasks require multiple employees

Information Security Frameworks

- **ISO/IEC 27000:** Guidelines on information security management
- **Zachman Framework:** Enterprise architecture model
- **TOGAF:** Enterprise information architecture
- **DoDAF:** DoD technologies integration view
- **MODAF:** British MOD viewpoint
- **SABSA:** Security framework based on risk
- **CobiT:** Control objectives for information technology
- **NIST SP 800-53:** Security controls framework
- **ITIL:** Managing IT service processes
- **Six Sigma:** Process improvement methodologies

Security Framework and Methodologies Deep Dive

- **Capability Maturity Model Integration (CMMI):** Process improvement; 5 maturity levels
- **Approach:** Top-Down vs. Bottom-Up initiative

Security Program Life Cycle

1. **Plan and Organize:** Risk assessment, management approval, asset management
2. **Implement:** Solutions, training, access controls
3. **Operate and Maintain:** Audits, SLA management
4. **Monitor and Evaluate:** Security goal reviews, improvement plans

The Pillars of Risk Assessment

- Determine asset value & vulnerability
- **Goals of Risk Assessment:**

> Asset Identification
>
> Threat Calculations: Likelihood impact balance
>
> Countermeasure Costs

Quantitative vs. Qualitative Risk Analysis

- **Quantitative Analysis:** Monetary values, Single Loss Expectancy (SLE), and Annual Loss Expectancy (ALE)
- **Qualitative Analysis:** Subjectivity, experience-based, organizational techniques

Choosing and Implementing Safeguards

Cost/Benefit Safeguard Selection: Weighing costs against potential losses

Total vs. Residual Risk: The effectiveness of implemented countermeasures

Handling Risk: Reduction, Avoidance, Transfer, Mitigation, Acceptance

Risk Management Principles

- **Risk Management Policy & Team:** Senior management commitment, objectives, roles, and monitoring processes

Building a Robust Security Policy

- **Types:** Organizational, System-specific, Issue-specific, Regulatory, Advisory, Informative
- **Completing the Policy Cycle:**

> **Standards and Baselines:** Tactical implementation
>
> **Guidelines and Procedures:** Recommendations and detailed actions
>
> **Information Classification Life Cycle:** Data value-based protection levels

Roles, Responsibilities, and Security Protocols

1. **Governance Roles:** From board members to users

2. **Procedures:** Personnel security, hiring, termination, and agreements

3. **Security Training:** Awareness, technical training, and education importance

Effective Measurement and Budgeting

- **Security Budget:** Allocation based on risk and cost-benefit analysis
- **Metrics and Effectiveness:** Short and long-term trends, third-party analysis recommendations

Information Security Buzz

Discover more at our InfoSec Knowledge Hub