Comptia Study Guide

1. General Security Concepts (12%):

- **Security Controls:**
  - Administrative, technical, and physical controls
  - Preventive, detective, and corrective controls
  - Deterrent and compensating controls
- **Fundamental Security Concepts:**
  - Confidentiality, Integrity, and Availability (CIA)
  - Non-repudiation
  - Authentication, Authorization, and Accounting (AAA)
  - Gap analysis
  - Zero Trust architecture
- **Change Management Processes:**
  - Configuration management
  - Patch management
  - Change control documentation
- **Cryptographic Solutions:**
  - Symmetric vs. asymmetric encryption
  - Hashing algorithms
  - Digital signatures
  - Public Key Infrastructure (PKI)

2. Threats, Vulnerabilities, and Mitigations (22%):

- **Threat Actors and Motivations:**
  - Script kiddies, hacktivists, nation-states, insiders
  - Financial gain, espionage, disruption
- **Threat Vectors and Attack Surfaces:**
  - Phishing, malware, social engineering
  - Network, application, and physical attack surfaces
- **Types of Vulnerabilities:**
  - Zero-day vulnerabilities
  - Configuration weaknesses
  - Unpatched systems
- **Indicators of Malicious Activity:**
  - Anomalous network traffic
  - Unauthorized access attempts
  - Unusual system behavior
- **Mitigation Techniques:**
  - Firewalls, intrusion detection/prevention systems
  - Antivirus software
  - Security awareness training

3. Security Architecture (18%):

- **Architecture Models:**
  - Client-server, peer-to-peer, cloud computing

    - Service-oriented architecture (SOA)
- **Securing Enterprise Infrastructure:**
    - Network segmentation
    - Defense in depth
    - Endpoint security
- **Data Protection Strategies:**
    - Data loss prevention (DLP)
    - Encryption at rest and in transit
    - Access controls
- **Resilience and Recovery:**
    - Disaster recovery planning
    - Business continuity planning
    - Redundancy and failover mechanisms

4. Security Operations (28%):

- **Security Techniques for Computing Resources:**
    - Hardening systems
    - Patch management
    - Secure configurations
- **Asset Management:**
    - Inventory management
    - Asset tagging
    - Data classification
- **Vulnerability Management:**
    - Scanning and assessment
    - Remediation planning
    - Penetration testing
- **Security Monitoring:**
    - Log analysis
    - Security Information and Event Management (SIEM)
    - Alerting mechanisms
- **Enhancing Security Capabilities:**
    - Implementing new security technologies
    - Regular security assessments
    - Continuous improvement processes
- **Identity and Access Management:**
    - Multi-factor authentication
    - Role-based access control
    - Single sign-on (SSO)
- **Automation and Orchestration:**
    - Automated incident response
    - Security orchestration tools
    - Scripted tasks
- **Incident Response Activities:**
    - Preparation, detection, and analysis
    - Containment, eradication, and recovery
    - Post-incident activities

- **Data Sources for Investigations:**
  - System logs
  - Network traffic captures
  - Forensic data

5. Security Program Management and Oversight (20%):

- **Security Governance:**
  - Policies, standards, and procedures
  - Security frameworks (e.g., NIST, ISO)
  - Organizational roles and responsibilities
- **Risk Management Process:**
  - Risk assessment and analysis
  - Risk mitigation strategies
  - Risk monitoring and reporting
- **Third-Party Risk Management:**
  - Vendor assessments
  - Supply chain security
  - Contractual agreements

Security Compliance and Audits:

- Regulatory requirements (e.g., GDPR, HIPAA, PCI-DSS)
- Internal and external audits
- Compliance reporting

Security Awareness and Training:

- Phishing and social engineering awareness
- Secure coding practices
- Role-based security training

Legal and Ethical Considerations:

- Data privacy laws
- Ethics in cybersecurity
- Cybersecurity liability and legal consequences