Information Assurance & Security - Pointers to Review

Topic 1: Foundations of Information Assurance & Security

Core Concepts

- - CIA Triad: Confidentiality, Integrity, Availability
- - Authentication vs. Authorization
- - Malware types, phishing, social engineering, DoS attacks
- - Security Controls: Preventive, Detective, Corrective
- - Symmetric vs. Asymmetric Encryption
- - Importance of Security Policies
- - Risk Management Process: Identification, Assessment, Mitigation

Best Practices

- - Patch management and updates
- - MFA and strong passwords
- - Data backup and recovery
- - Principle of Least Privilege

Topic 2: Network Security & Access Controls

Network Security Essentials

- - Firewalls and their rules
- - IDS vs. IPS
- - VPN use for secure connections
- - DMZ architecture
- - WPA3: Wi-Fi security standard

Access Control Models

- - DAC, MAC, RBAC, ABAC distinctions

Authentication Mechanisms

- - SSO, Biometrics, Tokens, Smart Cards

Common Attacks

- - MITM, Packet Sniffing, Brute Force, ARP Spoofing, Session Hijacking

Topic 3: Security Policies, Procedures & Compliance

Policy Frameworks

- - Acceptable Use, Password, Remote Access, Data Classification Policies

- - Lifecycle: Create, Approve, Enforce, Review

Incident Response & Disaster Recovery

- - IR Lifecycle: Preparation, Detection, Containment, Recovery, Review

- - BCP vs. DRP definitions

Compliance & Standards

- - ISO 27001, NIST, HIPAA, GDPR overview

- - Auditing & Monitoring importance

Topic 4: Careers in Cybersecurity & Certification Pathways

Cybersecurity Roles

- - Cybersecurity Analyst: Threat monitoring

- - Penetration Tester: Vulnerability assessment

- - Security Engineer: Secure systems architecting

- - SOC Analyst: Incident response

Certifications

- - Security+, CISSP, CEH, CISM

Skills to Develop

- - Threat analysis, SIEM tools, policy writing, vulnerability scans

- - OSI model & Networking fundamentals