5.0 Security Program Management and Oversight

5.1 Summarize elements of effective security governance.

- **Guidelines**
- **Policies**
  - Acceptable use policy (AUP)
  - Information security policies
  - Business continuity
  - Disaster recovery
  - Incident response
  - Software development lifecycle (SDLC)
  - Change management
- **Standards**
  - Password
  - Access control
  - Physical security
  - Encryption
- **Procedures**
  - Change management
  - Onboarding/offboarding
  - Playbooks
- **External considerations**
  - Regulatory
  - Legal
  - Industry
  - Local/regional
  - National
  - Global
- **Monitoring and revision**
- **Types of governance structures**
  - Boards
  - Committees
  - Government entities
  - Centralized/decentralized
- **Roles and responsibilities for systems and data**
  - Owners
  - Controllers
  - Processors
  - Custodians/stewards

5.2 Explain elements of the risk management process.

- **Risk identification**
- **Risk assessment**
  - Ad hoc
  - Recurring
  - One-time
  - Continuous
- **Risk analysis**
  - Qualitative
  - Quantitative
  - Single loss expectancy (SLE)
  - Annualized loss expectancy (ALE)
  - Annualized rate of occurrence (ARO)
  - Probability
  - Likelihood
  - Exposure factor
  - Impact
- **Risk register**
  - Key risk indicators
  - Risk owners
  - Risk threshold
- **Risk tolerance**
- **Risk appetite**
  - Expansionary
  - Conservative
  - Neutral
- **Risk management strategies**
  - Transfer
  - Accept
    - Exemption
    - Exception
  - Avoid
  - Mitigate
- **Risk reporting**
- **Business impact analysis**
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Mean time to repair (MTTR)
  - Mean time between failures (MTBF)

5.3 Explain the processes associated with third-party risk assessment and management.

- **Vendor assessment**
  - Penetration testing
  - Right-to-audit clause
  - Evidence of internal audits
  - Independent assessments
  - Supply chain analysis
- **Vendor selection**
  - Due diligence
  - Conflict of interest
- **Agreement types**
  - Service-level agreement (SLA)
  - Memorandum of agreement (MOA)
  - Memorandum of understanding (MOU)
  - Master service agreement (MSA)
  - Work order (WO)/statement of work (SOW)
  - Non-disclosure agreement (NDA)
  - Business partners agreement (BPA)
- **Vendor monitoring**
- **Questionnaires**
- **Rules of engagement**

5.4 Summarize elements of effective security compliance.

- **Compliance reporting**
  - Internal
  - External
- **Consequences of non-compliance**
  - Fines
  - Sanctions
  - Reputational damage
  - Loss of license
  - Contractual impacts
- **Compliance monitoring**
  - Due diligence/care
  - Attestation and acknowledgement
  - Internal and external
  - Automation
- **Privacy**
  - Legal implications
    - Local/regional
    - National
    - Global
  - Data subject
  - Controller vs. processor
  - Ownership
  - Data inventory and retention
  - Right to be forgotten

5.5 Explain types and purposes of audits and assessments.

- **Attestation**
- **Internal**
  - Compliance
  - Audit committee
  - Self-assessments
- **External**
  - Regulatory
  - Examinations
  - Assessment
  - Independent third-party audit
- **Penetration testing**
  - Physical
  - Offensive
  - Defensive
  - Integrated
  - Known environment
  - Partially known environment
  - Unknown environment
  - Reconnaissance
    - Passive
    - Active

5.6 Given a scenario, implement security awareness practices.

- **Phishing**
  - Campaigns
  - Recognizing a phishing attempt
  - Responding to reported suspicious messages
- **Anomalous behavior recognition**
  - Risky
  - Unexpected
  - Unintentional
- **User guidance and training**
  - Policy/handbooks
  - Situational awareness
  - Insider threat
  - Password management
  - Removable media and cables
  - Social engineering
  - Operational security
  - Hybrid/remote work environments
- **Reporting and monitoring**
  - Initial
  - Recurring
- **Development**
- **Execution**