1.0 Governance, Risk, and Compliance

1.1 Given a set of organizational security requirements, implement the appropriate governance components.

- **Security program documentation**
  - Policies
  - Procedures
  - Standards
  - Guidelines
- **Security program management**
  - Awareness and training
    - Phishing
    - Security
    - Social engineering
    - Privacy
    - Operational security
    - Situational awareness
  - Communication
  - Reporting
  - Management commitment
  - Responsible, accountable, consulted, and informed (RACI) matrix
- **Governance frameworks**
  - Control Objectives for Information and Related Technologies (COBIT)
  - Information Technology Infrastructure Library (ITIL)
- **Change/configuration management**
  - Asset management life cycle
  - Configuration management database (CMDB)
  - Inventory
- **Governance risk and compliance (GRC) tools**
  - Mapping
  - Automation
  - Compliance tracking
  - Documentation
  - Continuous monitoring
- **Data governance in staging environments**
  - Production
  - Development
  - Testing
  - Quality assurance (QA)
  - Data life cycle management

1.2 Given a set of organizational security requirements, perform risk management activities.

- **Impact analysis**
  - Extreme but plausible scenarios
- **Risk assessment and management**
  - Quantitative vs. qualitative analysis
  - Risk assessment frameworks
  - Appetite/tolerance
  - Risk prioritization
  - Severity impact
  - Remediation
  - Validation
- **Third-party risk management**
  - Supply chain risk
  - Vendor risk
  - Subprocessor risk
- **Availability risk considerations**
  - Business continuity/disaster recovery
    - Testing
  - Backups
    - Connected
    - Disconnected
- **Confidentiality risk considerations**
  - Data leak response
  - Sensitive/privileged data breach
  - Incident response testing
  - Reporting
  - Encryption
- **Integrity risk considerations**
  - Remote journaling
  - Hashing
  - Interference
  - Antitampering
- **Privacy risk considerations**
  - Data subject rights
  - Data sovereignty
  - Biometrics
- **Crisis management**
- **Breach response**

1.3 Explain how compliance affects information security strategies.

- **Awareness of industry-specific compliance**
  - Healthcare
  - Financial
  - Government
  - Utilities
- **Industry standards**
  - Payment Card Industry Data Security Standard (PCI DSS)
  - International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 series
  - Digital Markets Act (DMA)
- **Security and reporting frameworks**
  - Benchmarks
  - Foundational best practices
  - System and Organization Controls 2 (SOC 2)
  - National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
  - Center for Internet Security (CIS)
  - Cloud Security Alliance (CSA)
- **Audits vs. assessments vs. certifications**
  - External
  - Internal
- **Privacy regulations**
  - General Data Protection Regulation (GDPR)
  - California Consumer Privacy Act (CCPA)
  - General Data Protection Law (LGPD)
  - Children's Online Privacy Act (COPPA)
- **Awareness of cross-jurisdictional compliance requirements**
  - e-discovery
  - Legal holds
  - Due diligence
  - Due care
  - Export controls
  - Contractual obligations

1.4 Given a scenario, perform threat-modeling activities.

- **Actor characteristics**
  - Motivation
    - Financial
    - Geopolitical
    - Activism
    - Notoriety
    - Espionage
  - Resources
    - Time
    - Money
  - Capabilities
    - Supply chain access
    - Vulnerability creation
    - Knowledge
    - Exploit creation
- **Attack patterns**
- **Frameworks**
  - MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)
  - Common Attack Pattern Enumeration and Classification (CAPEC)
  - Cyber Kill Chain
  - Diamond Model of Intrusion Analysis
  - Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE)
  - Open Web Application Security Project (OWASP)
- **Attack surface determination**
  - Architecture reviews
  - Data flows
  - Trust boundaries
  - Code reviews
  - User factors
  - Organizational change
    - Mergers
    - Acquisitions
    - Divestitures
    - Staffing changes
  - Enumeration/discovery
    - Internally and externally facing assets
    - Third-party connections
    - Unsanctioned assets/accounts
    - Cloud services discovery
    - Public digital presence
- **Methods**
  - Abuse cases
  - Antipatterns
  - Attack trees/graphs
- **Modeling applicability of threats to the organization/environment**
  - With an existing system in place
    - Selection of appropriate controls
  - Without an existing system in place

1.5 Summarize the information security challenges associated with artificial intelligence (AI) adoption.

- **Legal and privacy implications**
  - Potential misuse
  - Explainable vs. non-explainable models
  - Organizational policies on the use of AI
  - Ethical governance
- **Threats to the model**
  - Prompt injection
  - Insecure output handling
  - Training data poisoning
  - Model denial of service (DoS)
  - Supply chain vulnerabilities
  - Model theft
  - Model inversion
- **AI-enabled attacks**
  - Insecure plug-in design
  - Deep fake
    - Digital media
    - Interactivity
  - AI pipeline injections
  - Social engineering
  - Automated exploit generation
- **Risks of AI usage**
  - Overreliance
  - Sensitive information disclosure
    - To the model
    - From the model
  - Excessive agency of the AI
- **AI-enabled assistants/digital workers**
  - Access/permissions
  - Guardrails
  - Data loss prevention (DLP)
  - Disclosure of AI usage