4.0 Governance, Risk, and Compliance

4.1 Given a set of requirements, apply the appropriate risk strategies.

- **Risk assessment**
  - Likelihood
  - Impact
  - Qualitative vs. quantitative
  - Exposure factor
  - Asset value
  - Total cost of ownership (TCO)
  - Return on investment (ROI)
  - Mean time to recovery (MTTR)
  - Mean time between failure (MTBF)
  - Annualized loss expectancy (ALE)
  - Annualized rate of occurrence (ARO)
  - Single loss expectancy (SLE)
  - Gap analysis
- **Risk handling techniques**
  - Transfer
  - Accept
  - Avoid
  - Mitigate
- **Risk types**
  - Inherent
  - Residual
  - Exceptions
- **Risk management life cycle**
  - Identify
  - Assess
  - Control
    - People
    - Process
    - Technology
    - Protect
    - Detect
    - Respond
    - Restore
  - Review
  - Frameworks
- **Risk tracking**
  - Risk register
  - Key performance indicators
    - Scalability
    - Reliability
    - Availability
  - Key risk indicators
- **Risk appetite vs. risk tolerance**
  - Tradeoff analysis
  - Usability vs. security requirements
- **Policies and security practices**
  - Separation of duties
  - Job rotation
  - Mandatory vacation
  - Least privilege
  - Employment and termination procedures
  - Training and awareness for users
  - Auditing requirements and frequency

4.2 Explain the importance of managing and mitigating vendor risk.

- **Shared responsibility model (roles/responsibilities)**
  - Cloud service provider (CSP)
    - Geographic location
    - Infrastructure
    - Compute
    - Storage
    - Networking
    - Services
  - Client
    - Encryption
    - Operating systems
    - Applications
    - Data
- **Vendor lock-in and vendor lockout**
- **Vendor viability**
  - Financial risk
  - Merger or acquisition risk
- **Meeting client requirements**
  - Legal
  - Change management
  - Staff turnover
  - Device and technical configurations
- **Support availability**
- **Geographical considerations**
- **Supply chain visibility**
- **Incident reporting requirements**
- **Source code escrows**
- **Ongoing vendor assessment tools**
- **Third-party dependencies**
  - Code
  - Hardware
  - Modules
- **Technical considerations**
  - Technical testing
  - Network segmentation
  - Transmission control
  - Shared credentials

4.3 Explain compliance frameworks and legal considerations, and their organizational impact.

- **Security concerns of integrating diverse industries**
- **Data considerations**
  - Data sovereignty
  - Data ownership
  - Data classifications
  - Data retention
  - Data types
    - Health
    - Financial
    - Intellectual property
    - Personally identifiable information (PII)
  - Data removal, destruction, and sanitization
- **Geographic considerations**
  - Location of data
  - Location of data subject
  - Location of cloud provider
- **Third-party attestation of compliance**
- **Regulations, accreditations, and standards**
  - Payment Card Industry Data Security Standard (PCI DSS)
  - General Data Protection Regulation (GDPR)
  - International Organization for Standardization (ISO)
  - Capability Maturity Model Integration (CMMI)
  - National Institute of Standards and Technology (NIST)
  - Children's Online Privacy Protection Act (COPPA)
  - Common Criteria
  - Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR)
- **Legal considerations**
  - Due diligence
  - Due care
  - Export controls
  - Legal holds
  - E-discovery
- **Contract and agreement types**
  - Service-level agreement (SLA)
  - Master service agreement (MSA)
  - Non-disclosure agreement (NDA)
  - Memorandum of understanding (MOU)
  - Interconnection security agreement (ISA)
  - Operational-level agreement
  - Privacy-level agreement

4.4 Explain the importance of business continuity and disaster recovery concepts.

- **Business impact analysis**
  - Recovery point objective
  - Recovery time objective
  - Recovery service level
  - Mission essential functions
- **Privacy impact assessment**
- **Disaster recovery plan (DRP)/ business continuity plan (BCP)**
  - Cold site
  - Warm site
  - Hot site
  - Mobile site
- **Incident response plan**
  - Roles/responsibilities
  - After-action reports
- **Testing plans**
  - Checklist
  - Walk-through
  - Tabletop exercises
  - Full interruption test
  - Parallel test/simulation test