# 5.0 Governance, Risk, and Compliance

## 5.1 Compare and contrast various types of controls.

- **Category**
  - Managerial
  - Operational
  - Technical
- **Control type**
  - Preventive
  - Detective
  - Corrective
  - Deterrent
  - Compensating
  - Physical

## 5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.

- **Regulations, standards, and legislation**
  - General Data Protection Regulation (GDPR)
  - National, territory, or state laws
  - Payment Card Industry Data Security Standard (PCI DSS)
- **Key frameworks**
  - Center for Internet Security (CIS)
  - National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)/ Cybersecurity Framework (CSF)
  - International Organization for Standardization (ISO) 27001/27002/27701/31000
  - SSAE SOC 2 Type I/II
  - Cloud security alliance
  - Cloud control matrix
  - Reference architecture
- **Benchmarks /secure configuration guides**
  - Platform/vendor-specific guides
    - Web server
    - OS
    - Application server
    - Network infrastructure devices

## 5.3 Explain the importance of policies to organizational security.

- **Personnel**
  - Acceptable use policy
  - Job rotation
  - Mandatory vacation
  - Separation of duties
  - Least privilege
  - Clean desk space
  - Background checks
  - Non-disclosure agreement (NDA)
  - Social media analysis
  - Onboarding
  - Offboarding
  - User training
    - Gamification
    - Capture the flag
    - Phishing campaigns
      - Phishing simulations
    - Computer-based training (CBT)
    - Role-based training
- **Diversity of training techniques**
- **Third-party risk management**
  - Vendors
  - Supply chain
  - Business partners
  - Service level agreement (SLA)
  - Memorandum of understanding (MOU)
  - Measurement systems analysis (MSA)
  - Business partnership agreement (BPA)
  - End of life (EOL)
  - End of service life (EOSL)
  - NDA
- **Data**
  - Classification
  - Governance
  - Retention
- **Credential policies**
  - Personnel
  - Third-party
  - Devices
  - Service accounts
  - Administrator/root accounts
- **Organizational policies**
  - Change management
  - Change control
  - Asset management

## 5.4 Summarize risk management processes and concepts.

- **Risk types**
  - External
  - Internal
  - Legacy systems
  - Multiparty
  - IP theft
  - Software compliance/licensing
- **Risk management strategies**
  - Acceptance
  - Avoidance
  - Transference
    - Cybersecurity insurance
  - Mitigation
- **Risk analysis**
  - Risk register
  - Risk matrix/heat map
  - Risk control assessment
  - Risk control self-assessment
  - Risk awareness
  - Inherent risk
  - Residual risk
  - Control risk
  - Risk appetite
  - Regulations that affect risk posture
  - Risk assessment types
    - Qualitative
    - Quantitative
  - Likelihood of occurrence
  - Impact
  - Asset value
  - Single-loss expectancy (SLE)
  - Annualized loss expectancy (ALE)
  - Annualized rate of occurrence (ARO)
- **Disasters**
  - Environmental
  - Person-made
  - Internal vs. external
- **Business impact analysis**
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Mean time to repair (MTTR)
  - Mean time between failures (MTBF)
  - Functional recovery plans
  - Single point of failure
  - Disaster recovery plan (DRP)
  - Mission essential functions
  - Identification of critical systems
  - Site risk assessment

## 5.5 Explain privacy and sensitive data concepts in relation to security.

- **Organizational consequences of privacy and data breaches**
  - Reputation damage
  - Identity theft
  - Fines
  - IP theft
- **Notifications of breaches**
  - Escalation
  - Public notifications and disclosures
- **Data types**
  - Classifications
    - Public
    - Private
    - Sensitive
    - Confidential
    - Critical
    - Proprietary
  - Personally identifiable information (PII)
  - Health information
  - Financial information
  - Government data
  - Customer data
- **Privacy enhancing technologies**
  - Data minimization
  - Data masking
  - Tokenization
  - Anonymization
  - Pseudo-anonymization
- **Roles and responsibilities**
  - Data owners
  - Data controller
  - Data processor
  - Data custodian/steward
  - Data protection officer (DPO)
- **Information life cycle**
- **Impact assessment**
- **Terms of agreement**
- **Privacy notice**