1.0 General Security Concepts

1.1 Compare and contrast various types of security controls.

- **Categories**
  - Technical
  - Managerial
  - Operational
  - Physical
- **Control types**
  - Preventive
  - Deterrent
  - Detective
  - Corrective
  - Compensating
  - Directive

1.2 Summarize fundamental security concepts.

- **Confidentiality, Integrity, and Availability (CIA)**
- **Non-repudiation**
- **Authentication, Authorization, and Accounting (AAA)**
  - Authenticating people
  - Authenticating systems
  - Authorization models
- **Gap analysis**
- **Zero Trust**
  - Control Plane
    - Adaptive identity
    - Threat scope reduction
    - Policy-driven access control
    - Policy Administrator
    - Policy Engine
  - Data Plane
    - Implicit trust zones
    - Subject/System
    - Policy Enforcement Point
- **Physical security**
  - Bollards
  - Access control vestibule
  - Fencing
  - Video surveillance
  - Security guard
  - Access badge
  - Lighting
  - Sensors
    - Infrared
    - Pressure
    - Microwave
    - Ultrasonic
- **Deception and disruption technology**
  - Honeypot
  - Honeynet
  - Honeyfile
  - Honeytoken

1.3 Explain the importance of change management processes and the impact to security.

- **Business processes impacting security operation**
  - Approval process
  - Ownership
  - Stakeholders
  - Impact analysis
  - Test results
  - Backout plan
  - Maintenance window
  - Standard operating procedure
- **Technical implications**
  - Allow lists/deny lists
  - Restricted activities
  - Downtime
  - Service restart
  - Application restart
  - Legacy applications
  - Dependencies
- **Documentation**
  - Updating diagrams
  - Updating policies/procedures
- **Version control**

1.4 Explain the importance of using appropriate cryptographic solutions.

- **Public key infrastructure (PKI)**
  - Public key
  - Private key
  - Key escrow
- **Encryption**
  - Level
    - Full-disk
    - Partition
    - File
    - Volume
    - Database
    - Record
  - Transport/communication
  - Asymmetric
  - Symmetric
  - Key exchange
  - Algorithms
  - Key length
- **Tools**
  - Trusted Platform Module (TPM)
  - Hardware security module (HSM)
  - Key management system
  - Secure enclave
- **Obfuscation**
  - Steganography
  - Tokenization
  - Data masking
- **Hashing**
- **Salting**
- **Digital signatures**
- **Key stretching**
- **Blockchain**
- **Open public ledger**
- **Certificates**
  - Certificate authorities
  - Certificate revocation lists (CRLs)
  - Online Certificate Status Protocol (OCSP)
  - Self-signed
  - Third-party
  - Root of trust
  - Certificate signing request (CSR) generation
  - Wildcard