3.0 Security Architecture

3.1 Compare and contrast security implications of different architecture models.

- **Architecture and infrastructure concepts**
  - Cloud
    - Responsibility matrix
    - Hybrid considerations
    - Third-party vendors
  - Infrastructure as code (IaC)
  - Serverless
  - Microservices
  - Network infrastructure
    - Physical isolation
      - Air-gapped
    - Logical segmentation
    - Software-defined networking (SDN)
  - On-premises
  - Centralized vs. decentralized
  - Containerization
  - Virtualization
  - IoT
  - Industrial control systems (ICS)/supervisory control and data acquisition (SCADA)
  - Real-time operating system (RTOS)
  - Embedded systems
  - High availability
- **Considerations**
  - Availability
  - Resilience
  - Cost
  - Responsiveness
  - Scalability
  - Ease of deployment
  - Risk transference
  - Ease of recovery
  - Patch availability
  - Inability to patch
  - Power
  - Compute

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

- **Infrastructure considerations**
  - Device placement
  - Security zones
  - Attack surface
  - Connectivity
  - Failure modes
    - Fail-open
    - Fail-closed
  - Device attribute
    - Active vs. passive
    - Inline vs. tap/monitor
  - Network appliances
    - Jump server
    - Proxy server
    - Intrusion prevention system (IPS)/intrusion detection system (IDS)
    - Load balancer
    - Sensors
  - Port security
    - 802.1X
    - Extensible Authentication Protocol (EAP)
  - Firewall types
    - Web application firewall (WAF)
    - Unified threat management (UTM)
    - Next-generation firewall (NGFW)
    - Layer 4/Layer 7
- **Secure communication/access**
  - Virtual private network (VPN)
  - Remote access
  - Tunneling
    - Transport Layer Security (TLS)
    - Internet protocol security (IPSec)
  - Software-defined wide area network (SD-WAN)
  - Secure access service edge (SASE)
- **Selection of effective controls**

3.3 Compare and contrast concepts and strategies to protect data.

- **Data types**
  - Regulated
  - Trade secret
  - Intellectual property
  - Legal information
  - Financial information
  - Human- and non-human-readable
- **Data classifications**
  - Sensitive
  - Confidential
  - Public
  - Restricted
  - Private
  - Critical
- **General data considerations**
  - Data states
    - Data at rest
    - Data in transit
    - Data in use
  - Data sovereignty
  - Geolocation
- **Methods to secure data**
  - Geographic restrictions
  - Encryption
  - Hashing
  - Masking
  - Tokenization
  - Obfuscation
  - Segmentation
  - Permission restrictions

3.4 Explain the importance of resilience and recovery in security architecture.

- **High availability**
  - Load balancing vs. clustering
- **Site considerations**
  - Hot
  - Cold
  - Warm
  - Geographic dispersion
- **Platform diversity**
- **Multi-cloud systems**
- **Continuity of operations**
- **Capacity planning**
  - People
  - Technology
  - Infrastructure
- **Testing**
  - Tabletop exercises
  - Fail over
  - Simulation
  - Parallel processing
- **Backups**
  - Onsite/offsite
  - Frequency
  - Encryption
  - Snapshots
  - Recovery
  - Replication
  - Journaling
- **Power**
  - Generators
  - Uninterruptible power supply (UPS)