3.0 Architecture and Design

3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides.

- **Industry-standard frameworks and reference architectures**
  - Regulatory
  - Non-regulatory
  - National vs. international
  - Industry-specific frameworks
- **Benchmarks/secure configuration guides**
  - Platform/vendor-specific guides
    - Web server
    - Operating system
    - Application server
    - Network infrastructure devices
  - General purpose guides
- **Defense-in-depth/layered security**
  - Vendor diversity
  - Control diversity
    - Administrative
    - Technical
  - User training

3.2 Given a scenario, implement secure network architecture concepts.

- **Zones/topologies**
  - DMZ
  - Extranet
  - Intranet
  - Wireless
  - Guest
  - Honeynets
  - NAT
  - Ad hoc
- **Segregation/segmentation/isolation**
  - Physical
  - Logical (VLAN)
  - Virtualization
  - Air gaps
- **Tunneling/VPN**
  - Site-to-site
  - Remote access
- **Security device/technology placement**
  - Sensors
  - Collectors
  - Correlation engines
  - Filters
  - Proxies
  - Firewalls
  - VPN concentrators
  - SSL accelerators
  - Load balancers
  - DDoS mitigator
  - Aggregation switches
  - Taps and port mirror
- **SDN**

3.3 Given a scenario, implement secure systems design.

- **Hardware/firmware security**
  - FDE/SED
  - TPM
  - HSM
  - UEFI/BIOS
  - Secure boot and attestation
  - Supply chain
  - Hardware root of trust
  - EMI/EMP
- **Operating systems**
  - Types
    - Network
    - Server
    - Workstation
    - Appliance
    - Kiosk
    - Mobile OS
  - Patch management
  - Disabling unnecessary ports and services
  - Least functionality
  - Secure configurations
  - Trusted operating system
  - Application whitelisting/blacklisting
  - Disable default accounts/passwords
- **Peripherals**
  - Wireless keyboards
  - Wireless mice
  - Displays
  - WiFi-enabled MicroSD cards
  - Printers/MFDs
  - External storage devices
  - Digital cameras

CompTIA.

3.4 Explain the importance of secure staging deployment concepts.

- **Sandboxing**
- **Environment**
  - Development
  - Test
  - Staging
  - Production
- **Secure baseline**
- **Integrity measurement**

3.5 Explain the security implications of embedded systems.

- **SCADA/ICS**
- **Smart devices/IoT**
  - Wearable technology
  - Home automation
- **HVAC**
- **SoC**
- **RTOS**
- **Printers/MFDs**
- **Camera systems**
- **Special purpose**
  - Medical devices
  - Vehicles
  - Aircraft/UAV

3.6 Summarize secure application development and deployment concepts.

- **Development life-cycle models**
  - Waterfall vs. Agile
- **Secure DevOps**
  - Security automation
  - Continuous integration
  - Baselining
  - Immutable systems
  - Infrastructure as code
- **Version control and change management**
- **Provisioning and deprovisioning**
- **Secure coding techniques**
  - Proper error handling
  - Proper input validation
  - Normalization
  - Stored procedures
  - Code signing
  - Encryption
  - Obfuscation/camouflage
  - Code reuse/dead code
  - Server-side vs. client-side execution and validation
  - Memory management
  - Use of third-party libraries and SDKs
  - Data exposure
- **Code quality and testing**
  - Static code analyzers
  - Dynamic analysis (e.g., fuzzing)
  - Stress testing
  - Sandboxing
  - Model verification
- **Compiled vs. runtime code**

3.7 Summarize cloud and virtualization concepts.

- **Hypervisor**
  - Type I
  - Type II
  - Application cells/containers
- **VM sprawl avoidance**
- **VM escape protection**
- **Cloud storage**
- **Cloud deployment models**
  - SaaS
  - PaaS
  - IaaS
  - Private
  - Public
  - Hybrid
  - Community
- **On-premise vs. hosted vs. cloud**
- **VDI/VDE**
- **Cloud access security broker**
- **Security as a Service**

3.8 Explain how resiliency and automation strategies reduce risk.

- **Automation/scripting**
  - Automated courses of action
  - Continuous monitoring
  - Configuration validation
- **Templates**
- **Master image**
- **Non-persistence**
  - Snapshots
  - Revert to known state
  - Rollback to known configuration
  - Live boot media
- **Elasticity**
- **Scalability**
- **Distributive allocation**
- **Redundancy**
- **Fault tolerance**
- **High availability**
- **RAID**

3.9 Explain the importance of physical security controls.

- **Lighting**
- **Signs**
- **Fencing/gate/cage**
- **Security guards**
- **Alarms**
- **Safe**
- **Secure cabinets/enclosures**
- **Protected distribution/Protected cabling**
- **Airgap**
- **Mantrap**
- **Faraday cage**
- **Lock types**
- **Biometrics**
- **Barricades/bollards**
- **Tokens/cards**
- **Environmental controls**
  - HVAC
  - Hot and cold aisles
  - Fire suppression
- **Cable locks**
- **Screen filters**
- **Cameras**
- **Motion detection**
- **Logs**
- **Infrared detection**
- **Key management**