2.0 Security

2.1 Given a scenario, configure identity and access management.

- **Identification and authorization**
  - Privileged access management
  - Logical access management
  - Account life-cycle management
    - Provision and deprovision accounts
  - Access controls
    - Role-based
    - Discretionary
    - Non-discretionary
    - Mandatory
- **Directory services**
  - Lightweight directory access protocol (LDAP)
- **Federation**
- **Certificate management**
- **Multifactor authentication (MFA)**
- **Single sign-on (SSO)**
  - Security assertion markup language (SAML)
- **Public key infrastructure (PKI)**
- **Secret management**
- **Key management**

2.2 Given a scenario, secure a network in a cloud environment.

- **Network segmentation**
  - Virtual LAN (VLAN)/Virtual extensible LAN (VXLAN)/ Generic network virtualization encapsulation (GENEVE)
  - Micro-segmentation
  - Tiering
- **Protocols**
  - Domain name service (DNS)
    - DNS over HTTPS (DoH)/ DNS over TLS (DoT)
    - DNS security (DNSSEC)
  - Network time protocol (NTP)
    - Network time security (NTS)
  - Encryption
    - IPSec
    - Transport layer security (TLS)
    - Hypertext transfer protocol secure (HTTPS)
  - Tunneling
    - Secure Shell (SSH)
    - Layer 2 tunneling protocol (L2TP)/ Point-to-point tunneling protocol (PPTP)
    - Generic routing encapsulation (GRE)
- **Network services**
  - Firewalls
    - Stateful
    - Stateless
  - Web application firewall (WAF)
  - Application delivery controller (ADC)
  - Intrusion protection system (IPS)/ Intrusion detection system (IDS)
  - Data loss prevention (DLP)
  - Network access control (NAC)
  - Packet brokers
- **Log and event monitoring**
- **Network flows**
- **Hardening and configuration changes**
  - Disabling unnecessary ports and services
  - Disabling weak protocols and ciphers
  - Firmware upgrades
  - Control ingress and egress traffic
    - Allow list (previously known as whitelisting) or blocklist (previously known as blacklisting)
    - Proxy servers
  - Distributed denial of service (DDoS) protection

2.3 Given a scenario, apply the appropriate OS and application security controls.

- **Policies**
  - Password complexity
  - Account lockout
  - Application approved list (previously known as whitelisting)
  - Software feature
  - User/group
- **User permissions**
- **Antivirus/anti-malware/endpoint detection and response (EDR)**
- **Host-based IDS (HIDS)/ Host-based IPS (HIPS)**
- **Hardened baselines**
  - Single function
- **File integrity**
- **Log and event monitoring**
- **Configuration management**
- **Builds**
  - Stable
  - Long-term support (LTS)
  - Beta
  - Canary
- **Operating system (OS) upgrades**
- **Encryption**
  - Application programming interface (API) endpoint
  - Application
  - OS
  - Storage
  - Filesystem
- **Mandatory access control**
- **Software firewall**

2.4 Given a scenario, apply data security and compliance controls in cloud environments.

- **Encryption**
- **Integrity**
  - Hashing algorithms
  - Digital signatures
  - File integrity monitoring (FIM)
- **Classification**
- **Segmentation**
- **Access control**
- **Impact of laws and regulations**
  - Legal hold
- **Records management**
  - Versioning
  - Retention
  - Destruction
  - Write once read many
- **Data loss prevention (DLP)**
- **Cloud access security broker (CASB)**

2.5 Given a scenario, implement measures to meet security requirements.

- **Tools**
  - Vulnerability scanners
  - Port scanners
- **Vulnerability assessment**
  - Default and common credential scans
  - Credentialed scans
  - Network-based scans
  - Agent-based scans
  - Service availabilities
- **Security patches**
  - Hot fixes
  - Scheduled updates
  - Virtual patches
  - Signature updates
  - Rollups
- **Risk register**
- **Prioritization of patch application**
- **Deactivate default accounts**
- **Impacts of security tools on systems and services**
- **Effects of cloud service models on security implementation**

2.6 Explain the importance of incident response procedures.

- **Preparation**
  - Documentation
  - Call trees
  - Training
  - Tabletops
  - Documented incident types/categories
  - Roles and responsibilities
- **Incident response procedures**
  - Identification
    - Scope
  - Investigation
  - Containment, eradication, and recovery
    - Isolation
    - Evidence acquisition
    - Chain of custody
  - Post-incident and lessons learned
    - Root cause analysis