Domain 3:
Security Architecture and Engineering

3.1 Implement and manage engineering processes using secure design principles

3.2 Understand the fundamental concepts of security models

3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- Client-based systems
- Server-based systems
- Database systems
- Cryptographic systems
- Industrial Control Systems (ICS)
- Cloud-based systems
- Distributed systems
- Internet of Things (IoT)

3.6 Assess and mitigate vulnerabilities in web-based systems

3.7 Assess and mitigate vulnerabilities in mobile systems

3.8 Assess and mitigate vulnerabilities in embedded devices

3.9 Apply cryptography

- Cryptographic life cycle (e.g., key management, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves)
- Public Key Infrastructure (PKI)
- Key management practices
- Digital signatures
- Non-repudiation
- Integrity (e.g., hashing)
- Understand methods of cryptanalytic attacks
- Digital Rights Management (DRM)

3.10 Apply security principles to site and facility design

3.11 Implement site and facility security controls

- Wiring closets/intermediate distribution facilities
- Server rooms/data centers
- Media storage facilities
- Evidence storage
- Restricted and work area security
- Utilities and Heating, Ventilation, and Air Conditioning (HVAC)
- Environmental issues
- Fire prevention, detection, and suppression