Domain 7: Security Operations

7.1 Understand and support investigations

- Evidence collection and handling
- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics, and procedures

7.2 Understand requirements for investigation types

- Administrative
- Criminal
- Civil
- Regulatory
- Industry standards

7.3 Conduct logging and monitoring activities

- Intrusion detection and prevention
- Security Information and Event Management (SIEM)
- Continuous monitoring
- Egress monitoring

7.4 Securely provisioning resources

- Asset inventory
- Asset management
- Configuration management

7.5 Understand and apply foundational security operations concepts

- Need-to-know/least privileges
- Separation of duties and responsibilities
- Privileged account management
- Job rotation
- Information lifecycle
- Service Level Agreements (SLA)

7.6 Apply resource protection techniques

- Media management
- Hardware and software asset management

7.7 Conduct incident management

- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Lessons learned

7.8 Operate and maintain detective and preventative measures

- Firewalls
- Intrusion detection and prevention systems
- Whitelisting/blacklisting
- Third-party provided security services
- Sandboxing
- Honeypots/honeynets
- Anti-malware

7.9 Implement and support patch and vulnerability management

7.10 Understand and participate in change management processes

7.11 Implement recovery strategies

- Backup storage strategies
- Recovery site strategies
- Multiple processing sites
- System resilience, high availability, Quality of Service (QoS), and fault tolerance

7.12 Implement Disaster Recovery (DR) processes

- Response
- Personnel
- Communications
- Assessment
- Restoration
- Training and awareness

7.13 Test Disaster Recovery Plans (DRP)

- Read-through/tabletop
- Walkthrough
- Simulation
- Parallel
- Full interruption

7.14 Participate in Business Continuity (BC) planning and exercises

7.15 Implement and manage physical security

- Perimeter security controls
- Internal security controls

7.16 Address personnel safety and security concerns

- Travel
- Security training and awareness
- Emergency management
- Duress