

Domain 7 **Security Operations**

- 7.1 Understand and comply with investigations
- 7.2 Conduct logging and monitoring activities
- 7.3 Perform Configuration Management (CM) (e.g. provisioning, baselining, automation)
- 7.4 Apply foundational security operations concepts
- 7.5 Apply resource protection
- 7.6 Conduct incident management
- 7.7 Operate and maintain detective and preventative measures
- 7.8 Implement and support patch and vulnerability management
- 7.9 Understand and participate in change management processes
- 7.10 Implement recovery strategies
- 7.11 Implement Disaster Recovery (DR) processes
- 7.12 Test Disaster Recovery Plans (DRP)
- 7.13 Participate in Business Continuity (BC) planning and exercises
- 7.14 Implement and manage physical security
- 7.15 Address personnel safety and security concerns