Exam Domain to Course Chapter Mapping

Domain	Chapter and Module
Domain 1: Security Principles	
1.1 Understand the security concepts of information assurance	Chapter 1, Module 1
1.1.1 Confidentiality	Chapter 1, Module 1
1.1.2 Integrity	Chapter 1, Module 1
1.1.3 Availability	Chapter 1, Module 1
1.1.4 Authentication (e.g., methods of authentication, multi-factor authentication (MFA))	Chapter 1, Module 1
1.1.5 Non-repudiation	Chapter 1, Module 1
1.1.6 Privacy	Chapter 1, Module 1
1.2 Understand the risk management process	Chapter 1, Module 2
1.2.1 Risk management (e.g., risk priorities, risk tolerance)	Chapter 1, Module 2
1.2.2 Risk identification, assessment and treatment	Chapter 1, Module 2
1.3 Understand security controls	Chapter 1, Module 3
1.3.1 Technical controls	Chapter 1, Module 3
1.3.2 Administrative controls	Chapter 1, Module 3
1.3.3 Physical controls	Chapter 1, Module 3
1.4 Understand the (ISC)² Code of Ethics	Chapter 1, Module 5
1.4.1 Professional code of conduct	Chapter 1, Module 5
1.5 Understand governance processes	Chapter 1, Module 4
1.5.1 Policies	Chapter 1, Module 4
1.5.2 Procedures	Chapter 1, Module 4
1.5.3 Standards	Chapter 1, Module 4
1.5.4 Regulations and laws	Chapter 1, Module 4
Domain 2: Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts	
2.1 Understand business continuity (BC)	Chapter 2, Module 2
2.1.1 Purpose	Chapter 2, Module 2
2.1.2 Importance	Chapter 2, Module 2
2.1.3 Components	Chapter 2, Module 2
2.2 Understand disaster recovery (DR)	Chapter 2, Module 3
2.2.1 Purpose	Chapter 2, Module 3

2.2.2 Importance	Chapter 2, Module 3
2.2.3 Components	Chapter 2, Module 3
2.3 Understand incident response	Chapter 2, Module 1
2.3.1 Purpose	Chapter 2, Module 1
2.3.2 Importance	Chapter 2, Module 1
2.3.3 Components	Chapter 2, Module 1
Domain 3: Access Control Concepts	
3.1 Understand physical access controls	Chapter 3, Module 2
3.1.1 Physical security controls (e.g., badge systems, gate entry, environmental design)	Chapter 3, Module 2
3.1.2 Monitoring (e.g., security guards, closed-circuit television (CCTV), alarm systems, logs)	Chapter 3, Module 2
3.1.3 Authorized versus unauthorized personnel	Chapter 3, Module 1
3.2 Understand logical access controls	Chapter 3, Module 3
3.2.1 Principle of least privilege	Chapter 3, Module 1
3.2.2 Segregation of duties	Chapter 3, Module 1
3.2.3 Discretionary access control (DAC)	Chapter 3, Module 3
3.2.4 Mandatory access control (MAC)	Chapter 3, Module 3
3.2.5 Role-based access control (RBAC)	Chapter 3, Module 3
Domain 4: Network Security	
4.1 Understand computer networking	Chapter 4, Module 1
4.1.1 Networks (e.g. Open Systems Interconnection (OSI) model, Transmission Control Protocol/Internet Protocol (TCP/IP) model, Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), Wi-Fi)	Chapter 4, Module 1
4.1.2 Ports	Chapter 4, Module 1
4.1.3 Applications	Chapter 4, Module 1
4.2 Understand network (cyber) threats and attacks	Chapter 4, Module 2
4.2.1 Types of threats (e.g., distributed denial-of-service (DDoS), virus, worm, Trojan, on-path attack, side-channel)	Chapter 4, Module 2
4.2.2 Identification (e.g., intrusion detection system (IDS), host-based intrusion detection system (HIDS), network intrusion detection system (NIDS))	Chapter 4, Module 2
4.2.3 Prevention (e.g., antivirus, scans, firewalls, intrusion prevention system (IPS))	Chapter 4, Module 2
4.3 Understand network security infrastructure	Chapter 4, Module 3

4.3.1 On-premises (e.g., power, data center/closets, Heating, Ventilation, and Air Conditioning (HVAC), environmental, fire suppression, redundancy, memorandum of understanding (MOU)/ memorandum of agreement (MOA))	Chapter 4, Module 3
4.3.2 Design (e.g., network segmentation (demilitarized zone (DMZ), virtual local area network (VLAN), virtual private network (VPN), micro-segmentation), defense in depth, Network Access Control (NAC) (segmentation for embedded systems, Internet of Things (IoT))	Chapter 4, Module 3
4.3.3 Cloud (e.g., service-level agreement (SLA), managed service provider (MSP), Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), hybrid)	Chapter 4, Module 3
Domain 5: Security Operations	
5.1 Understand data security	Chapter 5, Module 1
5.1.1 Encryption (e.g., symmetric, asymmetric, hashing)	Chapter 5, Module 1
5.1.2 Data handling (e.g., destruction, retention, classification, labeling)	Chapter 5, Module 1
5.1.3 Logging and monitoring security events	Chapter 5, Module 1
5.2 Understand system hardening	Chapter 5, Module 2
5.2.1 Configuration management (e.g., baselines, updates, patches)	Chapter 5, Module 2
5.3 Understand best practice security policies	Chapter 5, Module 3
5.3.1 Data handling policy	Chapter 5, Module 3
5.3.2 Password policy	Chapter 5, Module 3
5.3.3 Acceptable Use Policy (AUP)	Chapter 5, Module 3
5.3.4 Bring your own device (BYOD) policy	Chapter 5, Module 3
5.3.5 Change management policy (e.g., documentation, approval, rollback)	Chapter 5, Module 3
5.3.6 Privacy policy	Chapter 5, Module 3
5.4 Understand security awareness training	Chapter 5, Module 4
5.4.1 Purpose/concepts (e.g., social engineering, password protection)	Chapter 5, Module 4
5.4.2 Importance	Chapter 5, Module 4