Part 1

Cybersecurity Introduction and Overview
→ 1.1. Introduction to cybersecurity
→ 1.2. Difference between information security and cybersecurity
→ 1.3. Cybersecurity objectives
→ 1.4. Cybersecurity roles
→ 1.5. Cybersecurity domains

Cybersecurity Concepts
→ 2.1. Risk
→ 2.2. Common attack types and vectors
→ 2.3. Policies and procedures
→ 2.4. Cybersecurity controls

Part 2

Security Architecture
→ 3.1. Overview of security architecture
→ 3.2. The OSI model
→ 3.3. Defense in depth
→ 3.4. Information flow control
→ 3.5. Isolation and segmentation
→ 3.6. Logging, monitoring and detection
→ 3.7. Encryption fundamentals, techniques and applications

Part 3

Security of Networks, Systems, Applications and Data
→ 4.1. Process controls—Risk assessment
→ 4.2. Process controls—Vulnerability management
→ 4.3. Process controls—Penetration testing
→ 4.4. Network security
→ 4.5. Operating system security
→ 4.6. Application security
→ 4.7. Data security

Part 4

Incident Response
→ 5.1. Event vs. incident
→ 5.2. Security incident response
→ 5.3. Investigations, legal holds, and preservation
→ 5.4. Forensics
→ 5.5. Disaster recovery and business continuity Security Implications and Adoption of Evolving Technology
→ 6.1. Current threat landscape

→ 6.2. Advanced persistent threats(APTs)
→ 6.3. Mobile technology—Vulnerabilities, threats, and risk
→ 6.4. Consumerization of IT and mobile devices
→ 6.5. Cloud and digital collaboration