Domain 1: Security and Risk Management

1.1 Understand and apply concepts of confidentiality, integrity and availability

1.2 Evaluate and apply security governance principles

- Alignment of security function to business strategy, goals, mission, and objectives
- Organizational processes (e.g., acquisitions, divestitures, governance committees)
- Organizational roles and responsibilities
- Security control frameworks
- Due care/due diligence
- Determine compliance requirements

1.3 Determine compliance requirements

- Contractual, legal, industry standards, and regulatory requirements
- Privacy requirements

1.4 Understand legal and regulatory issues that pertain to information security in a global context

- Cyber crimes and data breaches
- Licensing and intellectual property requirements
- Import/export controls
- Trans-border data flow
- Privacy

1.5 Understand, adhere to, and promote professional ethics

- (ISC)² Code of Professional Ethics
- Organizational code of ethics

1.6 Develop, document, and implement security policy, standards, procedures, and guidelines

1.7 Identify, analyze, and prioritize Business Continuity (BC) requirements

- Develop and document scope and plan
- Business Impact Analysis (BIA)

1.8 Contribute to and enforce personnel security policies and procedures

- Candidate screening and hiring
- Employment agreements and policies
- Onboarding and termination processes
- Vendor, consultant, and contractor agreements and controls
- Compliance policy requirements
- Privacy policy requirements

1.9 Understand and apply risk management concepts

- Identify threats and vulnerabilities
- Risk assessment/analysis
- Risk response
- Countermeasure selection and implementation
- Applicable types of controls (e.g., preventive, detective, corrective)
- Security Control Assessment (SCA)
- Monitoring and measurement
- Asset valuation
- Reporting
- Continuous improvement
- Risk frameworks

1.10 Understand and apply threat modeling concepts and methodologies

- Threat modeling methodologies
- Threat modeling concepts

1.11 Apply risk-based management concepts to the supply chain

- Risks associated with hardware, software, and services
- Third-party assessment and monitoring
- Minimum security requirements
- Service-level requirements

1.12 Establish and maintain a security awareness, education, and training program

- Methods and techniques to present awareness and training
- Periodic content reviews
- Program effectiveness evaluation