Domain 1: Security and Risk Management

1.1 - Understand, adhere to, and promote professional ethics

ISC2 Code of Professional Ethics

Organizational code of ethics

1.2 - Understand and apply security concepts

Confidentiality, integrity, and availability, authenticity and nonrepudiation

1.3 - Evaluate and apply security governance principles

Alignment of the 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

1.4 - Determine compliance and other requirements

Contractual, legal, industry standards, and regulatory requirements

Privacy requirements

1.5 - Understand legal and regulatory issues that pertain to information security in a holistic context

Cybercrimes and data breaches

Licensing and Intellectual Property (IP) requirements

Import/export controls

Transborder data flow

Privacy

1.6 - Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

1.7 - Develop, document, and implement security policy, standards, procedures, and guidelines

1.8 - Identify, analyze, and prioritize Business Continuity (BC) requirements

Business Impact Analysis (BIA)

Develop and document the scope and the plan

1.9 - Contribute to and enforce personnel security policies and procedures

Candidate screening and hiring

Employment agreements and policies

Onboarding, transfers, and termination processes

Vendor, consultant, and contractor agreements and controls

Compliance policy requirements

Privacy policy requirements

1.10 - 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)

Control assessments (security and privacy)

Monitoring and measurement

Reporting

Continuous improvement (e.g., Risk maturity modeling)

Risk frameworks

1.11 - Understand and apply threat modeling concepts and methodologies

1.12 - Apply Supply Chain Risk Management (SCRM) concepts

Risks associated with hardware, software, and services

Third-party assessment and monitoring

Minimum security requirements

Service level requirements

1.13 - Establish and maintain a security awareness, education, and training program

Methods and techniques to present awareness and training (e.g., social engineering, phishing, security champions, gamification)

Periodic content reviews

Program effectiveness evaluation