CERTIFIED INFORMATION SYSTEM SECURITY PROFESSIONAL

Professional Certification: Information System Security

Course Code: M013/25

Duration: 5 Days

Delivery Format: Hybrid

Target Audience:

Individuals who

- Are involved in managing and implementing information security.
- Need to demonstrate their expertise in areas like risk management, asset protection, and network security.

Program Outcomes:

Upon completion of this program, participants will be able to:

- Understand essential areas of information security, including risk management, asset protection, network security, and software safety.
- Develop practical skills in handling security assessments, incident response, and implementing security measures.
- Apply security frameworks and guidelines to ensure organizational compliance with legal and industry requirements.
- Dive into advanced security topics like encryption, secure system design, and network security to solve complex problems.

- Learn to continuously improve security measures through risk assessment, practice updates, and security awareness training.

Detailed Syllabus

Module 1: Security and Risk Management

Outcome: Participants will understand the fundamental concepts of security and risk management.

Topics:

1.1: Understand, adhere to, and promote professional ethics

- (ISC)² Code of Professional Ethics
- Organizational code of ethics scorecard for Scrum teams

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: 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

1.9: Identify, analyze, and prioritize Business Continuity (BC) requirements

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

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
- Periodic content reviews
- Program effectiveness evaluation

Activities:

- Present case studies involving ethical dilemmas in information security (e.g., data breach disclosure, employee privacy vs. security).
- Assign groups to develop a security policy on a specific topic (e.g., password policy, acceptable use policy, data breach response policy).

Assessments:

- A quiz focused on the (ISC)² Code of Professional Ethics and ethical decision-making in security.
- Participants analyze a real-world case study of a security breach or incident, identifying the root causes, the impact, and the lessons learned.

Module 2: Asset Security

Outcome: Participants will understand the concepts and practices of asset security.

Topics:

2.1: Understand, adhere to, and promote professional ethics

- Data classification
- Asset Classification

2.2: Establish information and asset handling requirements

- Information and asset ownership
- Asset inventory
- Asset management

2.3: Provision resources securely

2.4: Manage data lifecycle

- Data roles (i.e., owners, controllers, custodians, processors, users/subjects)
- Data collection
- Data location
- Data states

2.5: Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))

2.6: Determine data security controls and compliance requirements

- Scoping and tailoring
- Standards selection

- Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB))

Activities:

- Provide participants with a set of sample data (e.g., documents, emails, files) and have them classify it according to sensitivity levels (e.g., confidential, internal use only, public).
- Role-play scenarios involving the provisioning of resources (e.g., onboarding a new employee, setting up a server).

Assessments:

- Participants create an asset inventory document for a given scenario.
- Participants propose a data protection solution for a specific business need, justifying their choice of methods and technologies.

Module 3: Security Architecture and Engineering

Outcome: Participants will understand the fundamental concepts of security architecture and engineering.

Topics:

3.1: Research, implement and manage engineering processes using secure design principles

- Threat modeling
- Least privilege
- Defense in depth
- Secure defaults
- Fail securely
- Separation of Duties (SoD)
- Keep it simple
- Zero Trust
- Privacy by design
- Trust but verify
- Shared responsibility

3.2: Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)

3.3: Select controls based upon systems security requirements

3.4: Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

3.5: Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- Client-based systems
- Server-based systems
- Database systems
- Cryptographic systems
- Industrial Control Systems (ICS)
- Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- Distributed systems
- Internet of Things (IoT)
- Microservices
- Containerization
- Serverless
- Embedded systems
- High-Performance Computing (HPC) systems
- Edge computing systems
- Virtualized systems

3.6: Select and determine cryptographic solutions

- Cryptographic life cycle (e.g., keys, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)
- Public Key Infrastructure (PKI)
- Key management practices
- Digital signatures and digital certificates
- Non-repudiation
- Integrity (e.g., hashing)

3.7: Identify, analyze, and prioritize Business Continuity (BC) requirements

- Brute force
- Ciphertext only
- Known plaintext
- Frequency analysis

- Chosen ciphertext
- Implementation attacks
- Side-channel
- Fault injection
- Timing » Man-in-the-Middle (MITM)
- Pass the hash
- Kerberos exploitation
- Ransomware

3.8: Apply security principles to site and facility design

3.9: Design site and facility security control

- Wiring closets/intermediate distribution facilities
- Server rooms/data centers
- Media storage facilities
- Evidence storage
- Restricted and work area security
- Utilities and Heating, Ventilation, and Air Conditioning (HVAC)
- Environmental issues
- Fire prevention, detection, and suppression
- Power (e.g., redundant, backup)

Activities:

- Case Study Analysis: Analyze a real-world case of a security breach due to architectural vulnerabilities.
- Threat Modeling Workshop: Conduct a threat modeling exercise for a sample application.

Assessments:

- Quiz: On security models and secure design principles.
- Design Document: Submission of a secure system design document.

Module 4: Communication and Network Security

Outcome: Participants will understand the principles and implementation of communication and network security.

Topics:

4.1: Assess and implement secure design principles in network architectures

- Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- Internet Protocol (IP) networking (e.g., Internet Protocol Security (IPSec), Internet Protocol (IP) v4/6)
- Secure protocols
- Implications of multilayer protocols
- Converged protocols (e.g., Fiber Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP))
- Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))
- Wireless networks (e.g., Li-Fi, Wi-Fi, Zigbee, satellite)
- Cellular networks (e.g., 4G, 5G)
- Content Distribution Networks (CDN)

4.2: Secure network components

- Operation of hardware
- Transmission media
- Network Access Control (NAC) devices
- Endpoint security

4.3: Implement secure communication channels according to design

- Voice
- Multimedia collaboration
- Remote access
- Data communications
- Virtualized networks
- Third-party connectivity

Activities:

- Network Design Simulation: Design a secure network for an organization, including segmentation, firewalls, and intrusion detection systems.
- Protocol Analysis: Analyze network traffic using Wireshark to identify potential security vulnerabilities.

Assessments:

- Network Security Plan: Documentation of a secure network design.

- Protocol Vulnerability Report: Report on identified vulnerabilities in network protocols.

Module 5: Identity and Access Management (IAM)

Outcome: Participants will understand the principles and mechanisms of Identity and Access Management.

Topics:

5.1: Manage identification and authentication of people, devices, and services

- Identity Management (IdM) implementation
- Single/Multi-Factor Authentication (MFA)
- Accountability
- Session management
- Registration, proofing, and establishment of identity
- Federated Identity Management (FIM)
- Credential management systems
- Interface testing
- Breach attack simulations
- Compliance checks
- Just-In-Time (JIT)

5.2: Federated identity with a third-party service

- On-premise
- Cloud
- Hybrid

5.3: Implement and manage authorization mechanisms

- Role Based Access Control (RBAC)
- Rule based access control
- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Attribute Based Access Control (ABAC)
- Risk based access control

5.4: Manage the identity and access provisioning lifecycle

- Account access review (e.g., user, system, service)
- Provisioning and deprovisioning (e.g., on /off boarding and transfers)

- Role definition (e.g., people assigned to new roles)
- Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)

5.5: Implement authentication systems

- OpenID Connect (OIDC)/Open Authorization (Oauth)
- Security Assertion Markup Language (SAML)
- Kerberos
- Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)

Activities:

- IAM Design Workshop: Design an IAM system for a company, including user provisioning, authentication methods, and authorization controls.
- Authentication Configuration: Configure different authentication methods like MFA or Kerberos in a lab environment.

Assessments:

- IAM Policy Document: Create an IAM policy document for an organization.
- Authentication System Configuration: Assessment of configuring authentication systems.

Module 6: Security Assessment and Testing

Outcome: Participants will understand the strategies and techniques for security assessment and testing.

Topics:

6.1: Design and validate assessment, test, and audit strategies

- Internal
- External
- Third-party

6.2: Collect security process data (e.g., technical and administrative)

- Account management
- Management review and approval
- Key performance and risk indicators
- Backup verification data
- Training and awareness

- Disaster Recovery (DR) and Business Continuity (BC)

6.3: Conduct security control testing

- Vulnerability assessment
- Penetration testing
- Log reviews
- Synthetic transactions
- Code review and testing
- Misuse case testing
- Test coverage analysis
- Interface testing
- Breach attack simulations
- Compliance checks

6.4: Analyze test output and generate report

- Remediation
- Exception handling
- Ethical disclosure

6.5: Manage the identity and access provisioning lifecycle

- Internal
- External
- Third-party

Activities:

- Vulnerability Assessment Exercise: Conduct a vulnerability assessment on a sample web application.
- Penetration Testing Simulation: Perform a simulated penetration test on a network.

Assessments:

- Vulnerability Assessment Report: Report on identified vulnerabilities and recommendations.
- Penetration Testing Report: Report detailing the findings of a penetration test.

Module 7: Security Operations

Outcome: Participants will understand the fundamental principles and practices of security operations.

Topics:

7.1: Understand and comply with investigations

- Evidence collection and handling
- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics, and procedures
- Artifacts (e.g., computer, network, mobile device)

7.2: Apply foundational security operations concepts

- Need-to-know/least privilege
- Separation of Duties (SoD) and responsibilities
- Privileged account management
- Job rotation
- Service Level Agreements (SLAs)

7.3: Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)

7.4: Conduct logging and monitoring activities

- Intrusion detection and prevention
- Security Information and Event Management (SIEM)
- Continuous monitoring
- Egress monitoring
- Log management
- Threat intelligence (e.g., threat feeds, threat hunting)
- User and Entity Behaviour Analytics (UEBA)

7.5: Apply resource protection

- Media management
- Media protection techniques

7.6: Conduct incident management

- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Lessons learned

7.7: Operate and maintain detective and preventative measures

- Firewalls (e.g., next generation, web application, network)
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- Whitelisting/blacklisting
- Third-party provided security services
- Sandboxing
- Honeypots/honeynets
- Anti-malware
- Machine learning and Artificial Intelligence (AI) based tools

7.8: Implement and support patch and vulnerability management

7.9: Understand and participate in change management processes

7.10: Implement recovery strategies

- Backup storage strategies
- Recovery site strategies
- Multiple processing sites
- System resilience, High Availability (HA), Quality of Service (QoS), and fault tolerance

7.11: Implement Disaster Recovery (DR) processes

- Response
- Personnel
- Communications
- Assessment
- Restoration
- Training and awareness
- Lessons learned

7.12: Test Disaster Recovery Plans (DRP)

- Read-through/tabletop
- Walkthrough Simulation
- Parallel
- Full interruption

7.13: Participate in Business Continuity (BC) planning and exercises

7.14: Implement and manage physical security

- Perimeter security controls
- Internal security controls

7.15: Address personnel safety and security concerns

- Travel
- Security training and awareness
- Emergency management
- Duress

Activities:

- Incident Response Simulation: Simulate a security incident and have participants follow the incident response process.
- Log Analysis Exercise: Analyze security logs to identify potential threats and anomalies.

Assessments:

- Incident Report: Create a detailed incident report based on a simulated scenario.
- Log Analysis Report: Report on findings from analyzing security logs.

Module 8: Software Development Security

Outcome: Participants will understand the principles and practices of secure software development.

Topics:

8.1: Understand and integrate security in the Software Development Life Cycle (SDLC)

- Development methodologies
- Maturity models
- Operation and maintenance
- Change management
- Integrated Product Team (IPT)

8.2: Assess security impact of acquired software

- Commercial-off-the-shelf (COTS)
- Open source
- Third-party
- Managed services

8.3: Assess the effectiveness of software security

- Auditing and logging of changes

- Risk analysis and mitigation

8.4: Identify and apply security controls in software development ecosystems

- Programming languages
- Libraries
- Tool sets
- Integrated Development Environment (IDE)
- Runtime
- Continuous Integration and Continuous Delivery (CI/CD)
- Security Orchestration, Automation, and Response (SOAR)
- Software Configuration Management (SCM)
- Code repositories
- Application security testing

8.5: Define and apply secure coding guidelines and standards

- Security weaknesses and vulnerabilities at the source-code level
- Security of Application Programming Interfaces (APIs)
- Secure coding practices
- Software-defined security

Activities:

- Secure Code Review: Conduct a code review to identify security vulnerabilities.
- Threat Modeling for Software: Perform threat modeling on a software application.

Assessments:

- Secure Code Analysis Report: Report on identified vulnerabilities in code and remediation steps.
- Threat Model Document: Documentation of a threat model for a software application.