SPRINTZEAL
Empowering Professionals

INFORMATION SYSTEMS SECURITY ENGINEERING PROFESSIONAL

Course Agenda

Course Overview:

Program Overview

Sprintzeal's ISSEP (Information Systems Security Engineering Professional) Certification Training Course offers comprehensive knowledge and skills in designing, implementing, and managing secure information systems. Our Certification Training equips participants with comprehensive knowledge and skills aligned with industry standards. Through structured modules, participants delve into core concepts and hands-on exercises, ensuring a robust understanding of each domain. Covering five essential domains mandated by the governing body, this course provides participants with the expertise required to excel in the field of information systems security engineering. With experienced instructors and interactive sessions, this training prepares individuals for success in the certification exam and real-world scenarios.

Key Learning Outcomes:

- Proficiency in applying systems security engineering fundamentals and processes.
- Ability to manage security risks to systems and operations, aligning them with enterprise risk management.
- Competence in developing security planning, design, and architecture, incorporating defense-in-depth concepts.
- Skills in implementing, verifying, and validating security solutions, ensuring they meet stakeholder requirements.
- Expertise in developing secure operations, change management, and disposal strategies, fostering continuous communication and compliance.

Skills Learned:

- Mastery of systems security engineering fundamentals
- Proficiency in risk management principles and practices
- Expertise in designing secure information systems and architectures
- Ability to implement and validate security solutions effectively
- Skill in managing secure operations, change management, and system disposal processes

Topics Covered:

Domain 1: Systems Security Engineering Foundations (20%)

- Apply systems security engineering fundamentals
- Execute systems security engineering processes
- Integrate with system development methodology
- Design Trusted Systems and Networks (TSN)
- Establish risk context and stakeholder tolerance
- Participate in the acquisition process

SPRINTZEAL
Empowering Professionals

Module 1: Security Operations and Administration

Module 1.1 - Comply with codes of ethics

- ISC2 Code of Ethics
- Organizational code of ethics

Module 1.2 - Understand security concepts

- Confidentiality
- Integrity
- Availability
- Accountability
- Privacy
- Non-repudiation
- Least privilege
- Segregation of duties (SoD)

Module 1.3 - Identify and implement security controls

- Technical controls (e.j., session timeout, password aging)
- Physical controls (e.g., mantraps, cameras, locks)
- Administrative controls (e.g., security policies, standards, procedures, baselines)
- Assessing compliance
- Periodic audit and review

Domain 2: Risk Management (19%)

- Apply security risk management principles
- Address risk to system and operations
- Document risk findings and decisions
- Recommend and assess risk treatment options
- Align security risk management with ERM
- Integrate risk management throughout the lifecycle

Domain 3: Security Planning and Design (22%)

- Analyze organizational and operational environment
- Develop system requirements and architecture
- Capture stakeholder requirements and threats
- Incorporate defense-in-depth concepts
- Develop system security context and baseline
- Perform functional analysis and allocation

Domain 4: Systems Implementation, Verification, and Validation (21%)

- Implement and deploy security solutions
- Verify and validate security solutions
- Perform system security implementation and integration
- Support continuous monitoring and Incident Response (IR)
- Perform security validation to demonstrate stakeholder requirements

Domain 5: Secure Operations, Change Management, and Disposal (18%)

- Develop secure operations strategy
- Participate in change management and disposal process
- Develop secure maintenance strategy
- Audit decommissioning and disposal process
- Contribute to continuous communication with stakeholders
- Develop secure disposal strategy and procedures

Targeted Audience:

- Experience in information security or related fields.
- Familiarity with system development methodologies.
- Understanding of security concepts and compliance frameworks.
- Proficiency in technical areas like network security.
- Recommended: CISSP certification or equivalent experience.

Prerequisites

- Experience in information security or related fields.
- Familiarity with system development methodologies.
- Understanding of security concepts and compliance frameworks.
- Proficiency in technical areas like network security.
- Recommended: CISSP certification or equivalent experience.

About Sprintzeal's ISSEP Training Course

Sprintzeal's ISSEP Training Course offers in-depth coverage of the five key domains outlined by the governing body. Participants gain a solid foundation in systems security engineering, risk management, security planning and design, systems implementation, verification, and validation, as well as secure operations, change management, and disposal. Led by seasoned instructors, this course provides practical insights and hands-on exercises to prepare participants for the ISSEP certification exam and excel in their security engineering careers.