SPRINTZEAL
Empowering Professionals

INFORMATION SYSTEMS SECURITY ARCHITECTURE PROFESSIONAL

Course Agenda

Course Overview:

Certification Training Overview:

Sprintzeal's ISSAP (Information Systems Security Architecture Professional) Certification Training Course provides a comprehensive understanding of designing, implementing, and managing secure information systems. Aligned with industry standards, this training equips participants with the requisite knowledge and skills across six key domains mandated by the governing body. Through structured modules and hands-on exercises, participants gain expertise in architecting for governance, compliance, risk management, security modeling, infrastructure security, identity and access management, application security, and security operations architecture. With experienced instructors and interactive sessions, this course prepares individuals for success in the ISSAP certification exam and real-world security architecture challenges.

Key Learning Outcomes:

- Master principles of security architecture design and implementation.
- Assess legal, regulatory, and industry requirements.
- Manage risk effectively within security frameworks.
- Model security architectures to meet diverse system needs.
- Integrate technical security controls and monitoring solutions.

Skills Learned:

- Security architecture design and implementation proficiency.
- Risk management and compliance assessment skills.
- Modeling and integrating security architectures.
- Technical security control implementation expertise.
- Effective monitoring and incident response capabilities.

Topics Covered:

Module 1: Architect for Governance, Compliance, and Risk Management (17%)

- Understanding legal, regulatory, organizational, and industry requirements
- Risk identification, classification, assessment, and management
- Compliance with information security standards, guidelines, and contractual obligations
- Coordination with external entities for auditability and risk monitoring
- Designing for auditability and integrating security into the acquisition process
- Managing risk through recommendation and monitoring
- Designing security policies aligned with governance and compliance standards

Module 2: Security Architecture Modeling (15%)

- Exploring security architecture approaches, frameworks, and reference architectures
- Designing defense-in-depth architecture for robust security posture
- Securing shared services and integrating technical security controls
- Infrastructure monitoring and threat modeling for validating security architecture design
- Verification and validation of security architecture through functional testing
- Developing security blueprints and reference architectures
- Incorporating security configuration and network segmentation

Module 3: Infrastructure Security Architecture (21%)

- Developing comprehensive infrastructure security requirements
- Designing cryptographic solutions and secure network infrastructure
- Evaluating physical and environmental security requirements
- Securing management networks, industrial control systems (ICS), and databases
- Ensuring cloud workload security and firmware security for holistic protection
- Implementing security controls for operating systems and containers
- Integrating security into the software-defined perimeter and virtualized environments

Module 4: Identity and Access Management (IAM) Architecture (16%)

- Designing identity and access management lifecycle with trust relationships
- Implementing authentication methods and access control configurations
- Managing privileged access and ensuring accountability through auditing mechanisms
- Designing centralized and decentralized IAM architectures for effective access management
- Securing credential management and implementing access control protocols
- Designing secure authentication mechanisms and multi-factor authentication solutions
- Implementing role-based access control (RBAC) and attribute-based access control (ABAC)

Module 5: Architect for Application Security (13%)

- Integrating Software Development Life Cycle (SDLC) with application security architecture
- Determining application security capability requirements and strategy
- Implementing proactive controls for applications and assessing security controls
- Secure coding practices, cryptographic solutions, and secure communication integration
- Ensuring secure application development and deployment in various environments
- Designing secure APIs and secure software architecture patterns
- Implementing secure coding standards and guidelines

Module 6: Security Operations Architecture (18%)

- Gathering security operations requirements and designing information security monitoring
- Designing Business Continuity (BC) and resiliency solutions for seamless operations
- Implementing Incident Response (IR) management processes and validating BCP/DRP architecture
- Preparation, identification, containment, eradication, recovery, and lessons learned in incident response
- Ensuring continuous communication with stakeholders and maintaining security operations efficiency
- Implementing security incident and event management (SIEM) solutions
- Designing and implementing security orchestration, automation, and response (SOAR) processes

Targeted Audience:

- Information security architects.
- Security consultants.
- IT managers and directors.
- System architects.
- Security engineers.

Prerequisites

- Possess a minimum of two years of professional experience in architecture or security.
- Hold a recognized bachelor's degree in a related field, or possess equivalent work experience.
- Obtain the CISSP (Certified Information Systems Security Professional) certification or its equivalent.

About Sprintzeal's ISSAP Training Course

Sprintzeal's ISSAP (Information Systems Security Architecture Professional) Training Course is meticulously designed to equip participants with the expertise required to excel in information systems security architecture. With a focus on aligning with industry standards, this comprehensive course covers six essential domains mandated by the governing body. Participants delve into a structured curriculum that includes in-depth discussions, hands-on exercises, and practical scenarios, ensuring a robust understanding of each domain. Led by experienced instructors, this training prepares individuals not only for success in the certification exam but also for real-world challenges in the field of information security architecture.