INFOSECTRAIN

ISSAP

Certified Information Systems Security Architecture Professional

Exam Prep Training

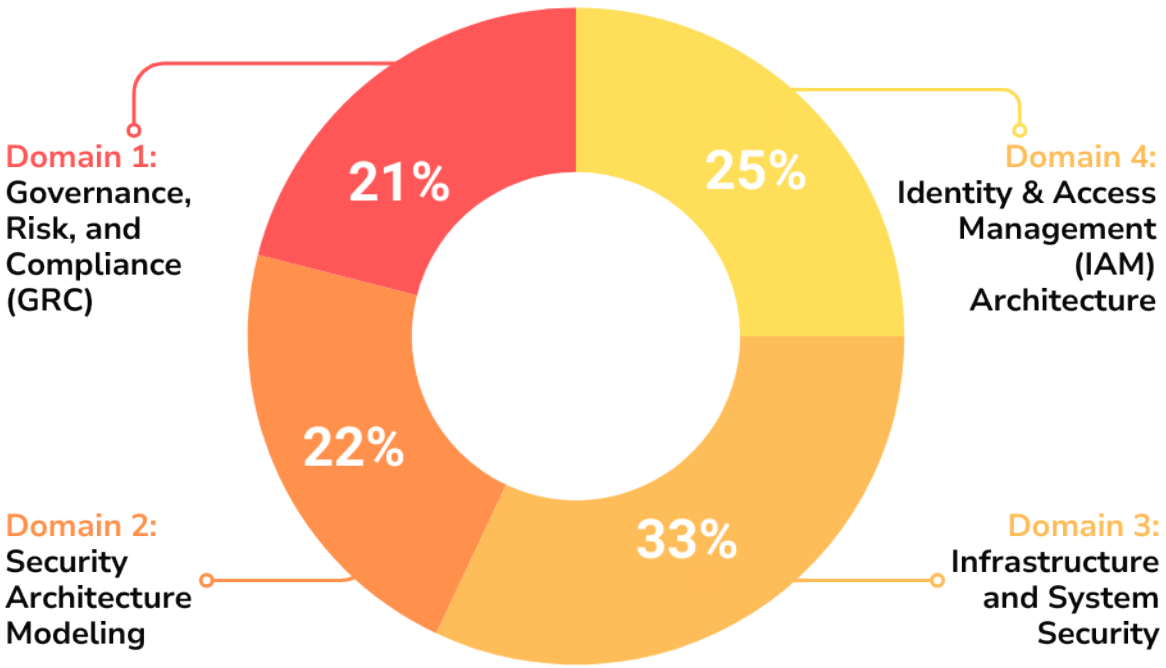
INFOSECTRAIN

Course Highlights

About Course

The information security architect plays a vital role to implement a sound security program in the organizations as an expert shouldering the role between a C-suite and upper managerial level. As an information security architect or analyst, this role involves executing diverse information security consultative and analytical processes. The ISSAP is an all-embracing certification that validates your technical skills in security architecture and grants the globally accepted credentials of chief security architect or analyst. This extensive certification evaluates your proficiency to develop, design and analyze various security solutions and instills skills to provide risk-based guidance to the higher management in addressing various organizational goals.

ISSAP Domains & Weightage



INFOSECTRAIN

Course Objectives

- Core concepts of access control systems, techniques, and access management architecture.
- Communications and networks architecture, considerations for security design and associated risks.
- Cryptography essentials, design considerations, and integrated cryptographic solutions including Public Key Infrastructure (PKI), API selection and more.
- Security architecture approach and analysis, design verification and validations.
- Disaster Recovery Planning (DRP), Business Continuity Planning (BCP), and Business Impact Analysis (BIA).
- Security strategies and recovery solutions.
- Physical security considerations, requirement assessment, and solutions evaluation.

INFOSECTRAIN

Target Audience

- System Architects
- Business Analysts
- System and Network Designers
- Chief Security Officers
- Chief Technology Officers

Pre-requisites

Candidates must be a CISSP in good standing and have two years cumulative, full-time experience in one or more of the six domains of the current ISSAP Exam Outline.

Or:

Candidates must have a minimum of seven years cumulative, full-time experience in two or more of the domains of the current ISSAP Exam Outline. Earning a post-secondary degree (bachelors or masters) in computer science, information technology (IT) or related fields or an additional credential from the ISC2 approved list may satisfy one year of the required experience. Part-time work and internships may also count towards the experience requirement.

INFOSECTRAIN

Exam Information

Exam Format	Multiple Choice Questions
Exam duration	3 hours
No. of Questions	125
Passing Score	700 out of 1000
Language	English

INFOSECTRAIN

Course Content

Domain 1 Governance, Risk, and Compliance (GRC) (21%)

1.1 Identify legal, regulatory, organizational, and industry requirements

- Applicable information security standards and guidelines
- Third-party and contractual obligations (e.g., supply chain, outsourcing, partners)
- Applicable sensitive/personal data standards, guidelines, and privacy regulations
- Resilient solutions

1.2 Architecting for governance, risk, and compliance (GRC)

- Identify key assets, business objectives, and stakeholders
- Design monitoring and reporting (e.g., vulnerability management, compliance audit)
- Design for auditability (e.g., determine regulatory, legislative, forensic requirements, segregation, high assurance systems)
- Incorporate risk assessment artifacts
- Advise risk treatment (e.g., mitigate, transfer, accept, avoid)

Domain 2 Security Architecture Modeling (22%)

2.1 Identify security architecture approach

- Scope (e.g., enterprise, cloud) and types (e.g., network, service-oriented architecture (SOA))
- Frameworks (e.g., The Open Group Architecture Framework (TOGAF), Sherwood Applied Business Security Architecture (SABSA), service-oriented modeling framework)
- Reference architectures and blueprints
- Threat modeling frameworks (e.g., Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE), Common Vulnerability Scoring System (CVSS), threat intelligence)

2.2 Verify and validate design (e.g., functional acceptance testing, regression)

- Results of threat modeling (e.g., threat vectors, impact, probability)
- Gaps
- Alternative solutions/mitigations/compensating controls
- Internal or external third-party (e.g., tabletop exercises, modeling and simulation, manual review of functions, peer review)
- Code review methodology (e.g., dynamic, manual, static, source composition analysis)

Domain 3 Infrastructure and System Security Architecture (32%)

3.1 Identify infrastructure and system security requirements

- Deployment model (e.g., On-premises, cloud-based, hybrid)
- Information technology (IT) and operational technology
- Physical security (e.g., perimeter protection and internal zoning, fire suppression)
- Infrastructure and system monitoring
- Infrastructure and system cryptography
- Application security (e.g., Requirements Traceability Matrix, security architecture documentation, secure coding)

3.2 Architect infrastructure and system security

- Physical security control set (e.g., cameras, doors, system controllers)
- Platform security (e.g., physical, virtual, container, firmware, operating system (OS))
- Network security (e.g., wired/wireless, public/private, Internet of Things (IoT), management, firewalls, airgaps, software defined perimeters, virtual private network (VPN), Internet Protocol Security (IPsec), Network Access Control (NAC), Domain Name System (DNS), Network Time Protocol (NTP), Voice over Internet Protocol (VoIP), Web Application Firewall (WAF))
- Storage security (e.g., direct attached, storage area network (SAN), network-attached storage (NAS), archival and removable media, encryption)
- Data repository security (e.g., access control, encryption, redaction, masking)

- Cloud security (e.g., public/private, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS))
- Operational technology (e.g., industrial control system (ICS), Internet of Things (IoT), supervisory control and data acquisition (SCADA))
- Endpoint security (e.g., bring your own device (BYOD), mobile, endpoint detection and response (EDR), host-based intrusion detection system (HIDS)/host-based intrusion prevention system (HIPS))
- Secure shared services (e.g., e-mail, Voice over Internet Protocol (VoIP), unified communications)
- Third-party integrations (e.g., internal/external, federation, application programming interface (API), virtual private network (VPN), Secure File Transfer Protocol (SFTP))
- Infrastructure monitoring
- Content monitoring (e.g., email, web, data, social media, data loss prevention (DLP))
- Out-of-band communications (e.g., incident response, information technology (IT) system management, Business Continuity (BC)/disaster recovery (DR))
- Evaluate applicability of security controls for system components (e.g., web client applications, proxy services, application services)

3.3 Architect infrastructure and system cryptographic solutions

- Determine cryptographic design considerations and constraints (e.g., technologies, lifecycle, computational capabilities, algorithms, attack in system)
- Determine cryptographic implementation (e.g., in-transit, in-use, at-rest)
- Plan key management lifecycle (e.g., generation, storage, distribution)

Domain 4 Identity and Access Management (IAM) Architecture (25%)

4.1 Architect identity lifecycle

- Establish identity and verify (e.g., physical, logical)
- Assign identifiers (e.g., to users, services, processes, devices, components)
- Identity provisioning and de-provisioning (e.g., joiners, movers, and leavers process)
- Identity management technologies

4.2 Architect identity authentication

- Define authentication approach (e.g., single-factor, multi-factor, risk-based elevation)
- Authentication protocols and technologies (e.g., Security Assertion Markup Language (SAML), Remote Authentication Dial-In User Service (RADIUS), Kerberos, Open Authorization (OAuth)
- Authentication control protocols and technologies (e.g., eXtensible Access Control Markup Language (XACML), Lightweight Directory Access Protocol (LDAP))
- Define trust relationships (e.g., federated, stand-alone)

4.3 Architect identity authorization

- Authorization concepts and principles (e.g., discretionary/mandatory, Separation of Duties (SoD), least privilege, interactive, non-interactive)
- Authorization models (e.g., physical, logical, administrative)

- Authorization process and workflow (e.g., governance, issuance, periodic review, revocation, suspension)
- Roles, rights, and responsibilities related to system, application, and data access control (e.g., groups, Digital Rights Management (DRM), trust relationships)
- Management of privileged accounts (e.g., Privileged Access Management (PAM))
- Authorization approach (e.g., single sign-on (SSO), rule-based, role-based, attribute-based, token, certificate)

4.4 Architect identity accounting

- Determine accounting, analysis, and forensic requirements
- Define audit events
- Establish audit log alerts and notifications
- Log management (e.g., log data retention, log data integrity)
- Log analysis and reporting
- Comply with policies and regulations (e.g., PCI-DSS, FISMA, HIPAA, GDPR)

INFOSECTRAIN

Happy Learners Across the World

Muhammad Akther
United Arab Emirates

The effort in teaching the concepts was commendable. Thank you, InfosecTrain, for your dedication to quality training in the ISSAP course!

Kunal Kumar
Singapore

Overall the ISSAP certification training was good. Trainer was well prepared with the content and target was to prepare for exam.

Himanshu Gupta
Spain

An excellent experience with engaging content! The ISSAP certification course offered valuable insights that will benefit my career immensely.

Md Faizuddin Siddiqui
United Arab Emirates

A professional and informative training experience! This ISSAP course exceeded my expectations and prepared me well for the challenges ahead.

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on