ISSAP®

Information Systems Security Architecture Professional

ISC2 Certification

Certification **Exam Outline**

Effective Date: August 1, 2025




ISC2

About ISSAP

The Information Systems Security Architecture Professional (ISSAP) is a security leader who specializes in designing security solutions and providing management with risk-based guidance to meet organizational goals. ISSAPs facilitate the alignment of security solutions within the organizational context (e.g., vision, mission, strategy, policies, requirements, change, and external factors).

The broad spectrum of topics included in the ISSAP Common Body of Knowledge (CBK®) ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following four domains:

- Governance, Risk, and Compliance (GRC)
- Security Architecture Modeling
- Infrastructure and System Security Architecture
- Identity and Access Management (IAM) Architecture

Experience Requirements

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

Accreditation

The ISSAP is in compliance with the stringent requirements of the ANSI National Accreditation Board (ANAB) ISO/IEC Standard 17024.

Job Task Analysis (JTA)

ISC2 has an obligation to its membership to maintain the relevancy of the ISSAP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by ISSAP credential holders. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing information security professionals.

ISSAP Examination Information

Length of exam	3 hours
Number of items	125
Item format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English
Testing center	Pearson VUE Testing Center

ISSAP Examination Weights

Domains	Weight
1. Governance, Risk, and Compliance (GRC)	21%
2. Security Architecture Modeling	22%
3. Infrastructure and System Security	32%
4. Identity and Access Management (IAM) Architecture	25%
Total:	**100%**

Domain 1: Governance, Risk, and Compliance (GRC)

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

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

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))

Domain 3: Infrastructure and System Security Architecture

- 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

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)

Domain 4: Identity and Access Management (IAM) Architecture

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)

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at **www.ISC2.org/certifications/references**.

Examination Policies and Procedures

ISC2 recommends that ISSAP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at **www.ISC2.org/Register-for-Exam**.

Legal Info

For any questions related to **ISC2's policies**, please contact the ISC2 Legal Department at legal@isc2.org.

Any Questions?

Contact ISC2 Candidate Services in your region:

Americas Tel: +1.866.331.ISC2 (4722), press 1
Email: membersupport@isc2.org

Asia-Pacific Tel: +(852) 5803-5662
Email: isc2asia@isc2.org

Europe, Middle East and Africa Tel: +44 (0)203-960-7800
Email: info-emea@isc2.org

ISC2