CISSP®

ISSAP®

Certified Information Systems Security Professional

Architecture

Certification **Exam Outline**

Effective Date: October 14, 2020

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

About CISSP-ISSAP

The Information Systems Security Architecture Professional (ISSAP) is a CISSP 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 six domains:

- Architect for Governance, Compliance, and Risk Management
- Security Architecture Modeling
- Infrastructure Security
- Identity and Access Management Architecture
- Architect for Application Security
- Security Operations Architecture

Experience Requirements

Candidates must be a CISSP in good standing and have two years cumulative paid work experience in one or more of the six domains of the CISSP-ISSAP CBK. You can learn more about CISSP-ISSAP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/CISSP-ISSAP/experience-requirements.

Accreditation

CISSP-ISSAP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

(ISC)² has an obligation to its membership to maintain the relevancy of the CISSP-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.

CISSP-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

CISSP-ISSAP Examination Weights

Domains	Weight
1. Architect for Governance, Compliance and Risk Management	17%
2. Security Architecture Modeling	15%
3. Infrastructure Security Architecture	21%
4. Identity and Access Management (IAM) Architecture	16%
5. Architect for Application Security	13%
6. Security Operations Architecture	18%
Total:	**100%**

Domain 1: Architect for Governance, Compliance and Risk Management

1.1 Determine legal, regulatory, organizational and industry requirements

- Determine applicable information security standards and guidelines
- Identify third-party and contractual obligations (e.g., supply chain, outsourcing, partners)
- Determine applicable sensitive/personal data standards, guidelines and privacy regulations
- Design for auditability (e.g., determine regulatory, legislative, forensic requirements, segregation, high assurance systems)
- Coordinate with external entities (e.g., law enforcement, public relations, independent assessor)

1.2 Manage Risk

- Identify and classify risks
- Assess risk
- Recommend risk treatment (e.g., mitigate, transfer, accept, avoid)
- Risk monitoring and reporting

Domain 2: Security Architecture Modeling

2.1 Identify security architecture approach

- Types and scope (e.g., enterprise, network, Service-Oriented Architecture (SOA), cloud, Internet of Things (IoT), Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA))
- Frameworks (e.g., Sherwood Applied Business Security Architecture (SABSA), Service-Oriented Modeling Framework (SOMF))
- Reference architectures and blueprints
- Security configuration (e.g., baselines, benchmarks, profiles)
- Network configuration (e.g., physical, logical, high availability, segmentation, zones)

2.2 Verify and validate design (e.g., Functional Acceptance Testing (FAT), regression)

- Validate results of threat modeling (e.g., threat vectors, impact, probability)
- Identify gaps and alternative solutions
- Independent Verification and Validation (IV&V) (e.g., tabletop exercises, modeling and simulation, manual review of functions)

Domain 3: Infrastructure Security Architecture

3.1 Develop infrastructure security requirements

- On-premise, cloud-based, hybrid
- Internet of Things (IoT), zero trust

3.2 Design defense-in-depth architecture

- Management networks
- Industrial Control Systems (ICS) security
- Network security
- Operating systems (OS) security
- Database security
- Container security
- Cloud workload security
- Firmware security
- User security awareness considerations

3.3 Secure shared services (e.g., wireless, e-mail, Voice over Internet Protocol (VoIP), Unified Communications (UC), Domain Name System (DNS), Network Time Protocol (NTP))

3.4 Integrate technical security controls

- Design boundary protection (e.g., firewalls, Virtual Private Network (VPN), airgaps, software defined perimeters, wireless, cloud-native)
- Secure device management (e.g., Bring Your Own Device (BYOD), mobile, server, endpoint, cloud instance, storage)

3.5 Design and integrate infrastructure monitoring

- Network visibility (e.g., sensor placement, time reconciliation, span of control, record compatibility)
- Active/Passive collection solutions (e.g., span port, port mirroring, tap, inline, flow logs)
- Security analytics (e.g., Security Information and Event Management (SIEM), log collection, machine learning, User Behavior Analytics (UBA))

Domain 3: Infrastructure Security Architecture

3.6 Design infrastructure cryptographic solutions

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

3.7 Design secure network and communication infrastructure (e.g., Virtual Private Network (VPN), Internet Protocol Security (IPsec), Transport Layer Security (TLS))

3.8 Evaluate physical and environmental security requirements

- Map physical security requirements to organizational needs (e.g., perimeter protection and internal zoning, fire suppression)
- Validate physical security controls

Domain 4: Identity and Access Management (IAM) Architecture

4.1 Design identity management and lifecycle

- Establish and verify identity
- Assign identifiers (e.g., to users, services, processes, devices)
- Identity provisioning and de-provisioning
- Define trust relationships (e.g., federated, stand-alone)
- Define authentication methods (e.g., Multi-Factor Authentication (MFA), risk-based, location-based, knowledge-based, object-based, characteristics-based)
- Authentication protocols and technologies (e.g., Security Assertion Markup Language (SAML), Remote Authentication Dial-In User Service (RADIUS), Kerberos)

4.2 Design access control management and lifecycle

- Access control concepts and principles (e.g., discretionary/mandatory, segregation/Separation of Duties (SoD), least privilege)
- Access control configurations (e.g., physical, logical, administrative)
- Authorization process and workflow (e.g., governance, issuance, periodic review, revocation)
- 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
- Authorization (e.g., Single Sign-On (SSO), rule-based, role-based, attribute- based)

4.3 Design identity and access solutions

- Access control protocols and technologies (e.g., eXtensible Access Control Markup Language (XACML), Lightweight Directory Access Protocol (LDAP))
- Credential management technologies (e.g., password management, certificates, smart cards)
- Centralized Identity and Access Management (IAM) architecture (e.g., cloud-based, on-premise, hybrid)
- Decentralized Identity and Access Management (IAM) architecture (e.g., cloud-based, on-premise, hybrid)
- Privileged Access Management (PAM) implementation (for users with elevated privileges)
- Accounting (e.g., logging, tracking, auditing)

Domain 5: Architect for Application Security

5.1 Integrate Software Development Life Cycle (SDLC) with application security architecture (e.g., Requirements Traceability Matrix (RTM), security architecture documentation, secure coding)

- Assess code review methodology (e.g., dynamic, manual, static)
- Assess the need for application protection (e.g., Web Application Firewall (WAF), anti-malware, secure Application Programming Interface (API), secure Security Assertion Markup Language (SAML))
- Determine encryption requirements (e.g., at-rest, in-transit, in-use)
- Assess the need for secure communications between applications and databases or other endpoints
- Leverage secure code repository

5.2 Determine application security capability requirements and strategy (e.g., open source, Cloud Service Providers (CSP), Software as a Service (SaaS)/Infrastructure as a Service (IaaS)/ Platform as a Service (PaaS) environments)

- Review security of applications (e.g., custom, Commercial Off-the-Shelf (COTS), in-house, cloud)
- Determine application cryptographic solutions (e.g., cryptographic Application Programming Interface (API), Pseudo Random Number Generator (PRNG), key management)
- Evaluate applicability of security controls for system components (e.g., mobile and web client applications; proxy, application, and database services)

5.3 Identify common proactive controls for applications (e.g., Open Web Application Security Project (OWASP))

Domain 6: Security Operations Architecture

6.1 Gather security operations requirements (e.g., legal, compliance, organizational, and business requirements)

6.2 Design information security monitoring (e.g., Security Information and Event Management (SIEM), insider threat, threat intelligence, user behavior analytics, Incident Response (IR) procedures)

- Detection and analysis
- Proactive and automated security monitoring and remediation (e.g., vulnerability management, compliance audit, penetration testing)

6.3 Design Business Continuity (BC) and resiliency solutions

- Incorporate Business Impact Analysis (BIA)
- Determine recovery and survivability strategy
- Identify continuity and availability solutions (e.g., cold, warm, hot, cloud backup)
- Define processing agreement requirements (e.g., provider, reciprocal, mutual, cloud, virtualization)
- Establish Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Design secure contingency communication for operations (e.g., backup communication channels, Out-of-Band (OOB))

6.4 Validate Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP) architecture

6.5 Design Incident Response (IR) management

- Preparation (e.g., communication plan, Incident Response Plan (IRP), training)
- Identification
- Containment
- Eradication
- Recovery
- Review lessons learned

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

(ISC)² 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 (ISC)²'s policies, please contact the (ISC)² Legal Department at legal@isc2.org.

Any Questions?

(ISC)² Americas
Tel: +1-866-331-ISC2(4722)
Email: membersupport@isc2.org

(ISC)² Asia Pacific
Tel: +852-2850-6951
Email: membersupportapac@isc2.org

(ISC)² EMEA
Tel: +44-203-960-7800
Email: membersupportemea@isc2.org