CISSP®

ISSAP®

Certified Information Systems Security Professional

Architecture

Certification **Exam Outline**

Effective Date: July 2017

(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:

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

Experience Requirements

Candidates must be a CISSP in good standing and have 2 years cumulative paid full-time work experience in 1 or more of the 6 domains of the CISSP-ISSAP CBK.

Accreditation

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 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 questions	125
Question 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. Identity and Access Management Architecture	19%
2. Security Operations Architecture	17%
3. Infrastructure Security	19%
4. Architect for Governance, Compliance, and Risk Management	16%
5. Security Architecture Modeling	14%
6. Architect for Application Security	15%
Total:	**100%**

Domain 1: Identity and Access Management Architecture

1.1 Design Identity Management and Lifecycle

- Identification and Authentication
- Centralized Identity and Access Management Architecture
- Decentralized Identity and Access Management Architecture
- Identity Provisioning Lifecycle (e.g., registration, issuance, revocation, validation)
- Authentication Protocols and Technologies (e.g., SAML, RADIUS, Kerberos, OATH)

1.2 Design Access Control Management and Lifecycle

- Application of Control Concepts and Principles (e.g., discretionary/mandatory, segregation/ separation of duties, rule of least privilege)
- Access Control Governance
- Access Control Configurations (e.g., physical, logical, administrative)
- Authorization Process and Workflow (e.g., 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)
- Authorization (e.g., single sign-on, rule-based, role-based, attribute-based)
- Accounting (e.g., logging, tracking, auditing)
- Access Control Protocols and Technologies (e.g., XACML, LDAP)
- Network Access Control

Domain 2: Security Operations Architecture

2.1 Determine Security Operation Capability Requirements and Strategy

- Determine Legal Imperatives
- Determine Organizational Drivers and Strategy
- Determine Organizational Constraints
- Map Current Capabilities to Organization Strategy
- Design Security Operations Strategy

2.2 Design Continuous Security Monitoring (e.g., SIEM, insider threat, enterprise log management, cyber crime, advanced persistent threat)

- Detection and Response
- Content Monitoring, Inspection, and Filtering (e.g., email, web, data, social media)
- Anomoly Detection (e.g., baseline, analytics, false positive reduction)

2.3 Design Continuity, Availability, and Recovery Solutions

- Incorporate Business Impact Analysis (BIA) Information (e.g., legal, financial, stakeholders)
- Determine Security Strategies for Availability and Recovery
- Design Continuity and Recovery Solution

2.4 Define Security Operations (e.g., interoperability, scalability, availability, supportability)

2.5 Integrate Physical Security Controls

- Assess Physical Security Requirements
- Integrate Physical Security Products and Systems
- Evaluate Physical Security Solutions (e.g., test, evaluate, implement)

2.6 Design Incident Management Capabilities

2.7 Secure Communications and Networks

- Design the Maintenance Plan for the Communication and Network Architecture
- Determine Communications Architecture
- Determine Network Architecture
- Communication and Network Policies
- Remote Access

Domain 3: Infrastructure Security

3.1 Determine Infrastructure Security Capability Requirements and Strategy

3.2 Design Layer 2/3 Architecture (e.g., access control segmentation, out-of-band management, OSI layers)

3.3 Secure Common Services (e.g., wireless, e-mail, VoIP, unified communications)

3.4 Architect Detective, Deterrent, Preventative, and Control Systems

- Design Boundary Protection (e.g., firewalls, VPNs, airgaps, BYOD, software defined perimeters)
- Secure Device Management (e.g., BYOD, mobile, server, endpoint)

3.5 Architect Infrastructure Monitoring

- Monitor Integration (e.g., sensor placement, time reconciliation, span of control, record compatibility)
- Active/Passive Solutions (e.g., span port, port mirroring, tap, inline)

3.6 Design Integrated Cryptographic Solutions (e.g., Public Key Infrastructure (PKI), identity system integration)

- Determine Usage (i.e., in transit, at rest)
- Define Key Management Lifecycle
- Identify Cryptographic Design Considerations and Constraints

Domain 4: Architect for Governance, Compliance, and Risk Management

4.1 Architect for Governance and Compliance

- Auditability (e.g., regulatory, legislative, forensic requirements, segregation, verifiability of high assurance systems)
- Secure Sourcing Strategy
- Apply Existing Information Security Standards and Guidelines (e.g., ISO/IEC, PCI, SOX, SOC2)
- Governing the Organizational Security Portfolio

4.2 Design Threat and Risk Management Capabilities

- Identify Security Design Considerations and Associated Risks
- Design for Compliance
- Assess Third Parties (e.g., auditing and risk registry)

4.3 Architect Security Solutions for Off-Site Data Use and Storage

- Cloud Service Providers
- Third Party
- Network Solutions Service Providers (NSSP)

4.4 Operating Environment (e.g., virtualization, cloud computing)

Domain 5: Security Architecture Modeling

5.1 Identify Security Architecture Approach (e.g., reference architectures, build guides, blueprints, patterns)

- Types and Scope (e.g., enterprise, network, SOA)
- Frameworks (e.g., Sherwood Applied Business Security Architecture (SABSA), Service-Oriented Modeling Framework (SOMF))
- Industrial Control Systems (ICS) (e.g., process automation networks, work interdependencies, monitoring requirements)
- Security Configuration (e.g., baselines)
- Network Configuration (e.g., physical, logical, high availability)
- Reference Architectures

5.2 Verify and Validate Design (e.g., POT, FAT, regression)

- Validate Threat Model (e.g., access control attacks, cryptanalytic attacks, network)
- Identification of Gaps and Alternative Solutions
- Independent Verification and Validation
- Evaluate Controls Against Threats and Vulnerabilities
- Validation of Design Against Reference Architectures

Domain 6: Architect for Application Security

6.1 Review Software Development Life Cycle (SDLC) Integration of Application Security Architecture (e.g., requirements traceability matrix, security architecture documentation, secure coding)

- » Assess When to Use Automated vs. Manual vs. Static Secure Code Reviews Based on Risk
- » Assess the Need for Web Application Firewalls (e.g., REST, API, SAML)
- » Review the Need for Encryption between Identity Providers at the Transport and Content Layers
- » Assess the Need for Secure Communications between Applications and Databases or other Endpoints
- » Leverage Secure Code Repository

6.2 Review Application Security (e.g., custom, commercial off-the-shelf (COTS), in-house cloud)

6.3 Determine Application Security Capability Requirements and Strategy (e.g., open source, cloud service providers, SaaS/IaaS providers)

6.4 Design Application Cryptographic Solutions (e.g., cryptographic API selection, PRNG selection, software-based key management)

6.5 Evaluate Application Controls Against Existing Threats and Vulnerabilities

6.6 Determine and Establish Application Security Approaches for all System Components (mobile, web, and thick client applications; proxy, application, and database services)

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/issap-cbk-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/exam-policies-procedures.

Legal Info

For any questions related to (ISC)²'s legal policies, please contact the (ISC)² Legal Department at legal@isc2.org.

Any Questions?

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Americas
Tel: +1.727.785.0189
Email: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 28506951
Email: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0)203 300 1625
Email: info-emea@isc2.org