CISSP®

Certified Information Systems Security Professional

ISSAP® Architecture

An (ISC)² Certification

Domain Refresh

Effective Date: October 14, 2020

*Please note: The **CISSP-ISSAP Exam Outline** is the official document outlining the domains, weights and subdomains of the certification exam. This document is intended as a supplementary resource only.*

CISSP-ISSAP Domain Refresh

On October 14, 2020, the domains for the (ISC)² CISSP-ISSAP® credential exam will be refreshed and the current CISSP-ISSAP is available on our website.

The content of the CISSP-ISSAP has been refreshed to reflect the most pertinent issues that cybersecurity architecture professionals currently face. Some topics have been updated while others have been realigned. The result is an exam that most accurately reflects best practices for developing, designing and analyzing security solutions.

As a result of the content refresh, the domain and subdomain names have been updated to describe the topics accurately. The weights for the domains have also changed. Please see the comparison table on the next page.

Domain Comparison

July 2017 – October 13, 2020	Effective October 14, 2020
Domain 1: Identity and Access Management Architecture	**Domain 1:** **Architect for Governance, Compliance, and Risk Management**
• Design Identity Management and Lifecycle • Design Access Control Management and Lifecycle	• **Determine legal, regulatory, organizational, and industry requirements** • **Manage risk**
Exam Weight: 19%	**Exam Weight: 17%**

July 2017 – October 13, 2020	Effective October 14, 2020
Domain 2: Security Operations Architecture	**Domain 2:** **Security Architecture Modeling**
• Determine Security Operation Capability Requirements and Strategy • Design Continuous Security Monitoring (e.g., SIEM, insider threat, enterprise log management, cyber crime, advanced persistent threat) • Design Continuity, Availability, and Recovery Solutions • Define Security Operations (e.g., interoperability, scalability, availability, supportability) • Integrate Physical Security Controls • Design Incident Management Capabilities • Secure Communications and Networks	• **Identify security architecture approach** • **Verify and validate design (e.g., Functional Acceptance Testing (FAT), regression)**
Exam Weight: 17%	**Exam Weight: 15%**

July 2017 – October 13, 2020	Effective October 14, 2020
Domain 3: Infrastructure Security	**Domain 3:** **Infrastructure Security Architecture**
• Determine Infrastructure Security Capability Requirements and Strategy • Design Layer 2/3 Architecture (e.g., access control segmentation, out-of-band management, OSI layers) • Secure Common Services (e.g., wireless, e-mail, VoIP, unified communications) • Architect Detective, Deterrent, Preventative, and Control Systems • Architect Infrastructure Monitoring • Design Integrated Cryptographic Solutions (e.g., Public Key Infrastructure (PKI), identity system integration)	• **Develop infrastructure security requirements** • **Design defense-in-depth architecture** • **Secure shared services (e.g., wireless, e-mail, Voice over Internet Protocol (VoIP), Unified Communications (UC),** • **Domain Name System (DNS), Network Time Protocol (NTP))** • **Integrate technical security controls** • **Design and integrate infrastructure monitoring** • **Design infrastructure cryptographic solutions** • **Design secure network and communication infrastructure (e.g., Virtual Private Network (VPN), Internet Protocol Security (IPsec), Transport Layer Security (TLS))** • **Evaluate physical and environmental security requirements**
Exam Weight: 19%	**Exam Weight: 21%**

July 2017 – October 13, 2020	Effective October 14, 2020
Domain 4: Architect for Governance, Compliance, and Risk Management	**Domain 4:** **Identity and Access Management (IAM) Architecture**
• Architect for Governance and Compliance • Design Threat and Risk Management Capabilities • Architect Security Solutions for Off-Site Data Use and Storage • Operating environment (e.g., virtualization, cloud computing)	• **Design identity management and lifecycle** • **Design access control management and lifecycle** • **Design identity and access solutions**
Exam Weight: 16%	**Exam Weight: 14%**

July 2017 – October 13, 2020	Effective October 14, 2020
Domain 5: Security Architecture Modeling	**Domain 5:** **Architect for Application Security**
• Identify Security Architecture Approach (e.g., reference architectures, build guides, blueprints, patterns) • Verify and Validate Design (e.g., POT, FAT, regression)	• **Integrate Software Development Life Cycle (SDLC) with application security architecture (e.g., Requirements Traceability Matrix (RTM), security architecture documentation, secure coding)** • **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)** • **Identify common proactive controls for applications (e.g., Open Web Application Security Project (OWASP))**
Exam Weight: 14%	**Exam Weight: 13%**

July 2017 – October 13, 2020	Effective October 14, 2020
Domain 6: Architect for Application Security	**Domain 6:** **Security Operations Architecture**
• Review Software Development Life Cycle (SDLC) Integration of Application Security Architecture (e.g., requirements traceability matrix, security architecture documentation, secure coding) • Review Application Security (e.g., custom, commercial off-the-shelf (COTS), in-house, cloud) • Determine Application Security Capability Requirements and Strategy (e.g., open source, cloud service providers, SaaS/IaaS providers) • Design Application Cryptographic Solutions (e.g., cryptographic API selection, PRNG selection, software-based key management) • Evaluate Application Controls Against Existing Threats and Vulnerabilities • Determine and establish application security approaches for all system components (mobile, web, and thick client applications; proxy, application, and database services)	• **Gather security operations requirements (e.g., legal, compliance, organizational, and business requirements)** • **Design information security monitoring (e.g., Security Information and Event Management (SIEM), insider threat, threat intelligence, user behavior analytics, Incident Response (IR) procedures)** • **Design Business Continuity (BC) and resiliency solutions** • **Validate Business Continuity Plan (BCP)/ Disaster Recovery Plan (DRP) architecture** • **Design Incident Response (IR) management**
Exam Weight: 15%	**Exam Weight: 18%**

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 CISSP-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 legal 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