CISSP®

Certified Information Systems Security Professional

ISSEP® Engineering

An (ISC)² Certification

Domain Refresh

Effective Date: November 13, 2020

*Please note: The **CISSP-ISSEP 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-ISSEP Domain Refresh

On November 13, 2020, the domains for the (ISC)² CISSP-ISSEP® credential exam will be refreshed.

The content of the CISSP-ISSEP will be refreshed to reflect the most pertinent issues that cybersecurity engineering professionals currently face. These enhancements are the result of a rigorous, methodical process that (ISC)² follows to routinely update its credential exams. This process ensures that the examinations and subsequent continuing professional education requirements encompass the topic areas relevant to the roles and responsibilities of today's practicing cybersecurity engineering professional.

The CISSP-ISSEP exam will be reduced to 125 items from 150. (ISC)² has decided to reduce the number of exam items from 125 operational and 25 pre-test items to 100 operational and 25 pre-test items. The testing time of three hours remains the same. The decision to reduce test length for the CISSP-ISSEP exam was made to maintain consistency across all (ISC)² exams

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 below.

Effective March 2018

#	Major Domains	Weights
1.	Security Engineering Principles	22%
2.	Risk Management	24%
3.	Security Planning, Design, and Implementation	22%
4.	Secure Operations, Maintenance, and Disposal	21%
5.	Systems Engineering Technical Management	11%
		100%

Effective November 13, 2020

#	Major Domains	Weights
1.	Systems Security Engineering Foundations	25%
2.	Risk Management	14%
3.	Security Planning and Design	30%
4.	Systems Implementation, Verification and Validation	14%
5.	Secure Operations, Change Management and Disposal	17%
		100%

Domain Comparison

March 2018 – November 12, 2020	Effective November 13, 2020
Domain 1: Security Engineering Principles	**Domain 1:** Systems Security Engineering Foundations
• General Security Principles • Security Risk Management Principles • System Resilience Principles • Vulnerability Management Principles	• **Apply systems security engineering fundamentals** • **Execute systems security engineering processes** • **Integrate with applicable system development methodology** • **Perform technical management** • **Participate in the acquisition process** • **Design Trusted Systems and Networks**
Exam Weight: 22%	**Exam Weight: 25%**
Domain 2: Risk Management	**Domain 2:** Risk Management
• Risk Management Process • Operational Risk Management	• **Apply security risk management principles** • **Address risk to system** • **Manage risk to operations**
Exam Weight: 24%	**Exam Weight: 14%**

Domain Comparison

Domain 3: Security Planning, Design and Implementation	**Domain 3:** **Security Planning and Design**
• Stakeholder Requirements Definition • Requirements Analysis • Systems Security Architecture and Design • Implementation, Integrations and Deployment of Systems or System Modifications. • Verification and Validation of System or Systems Modifications	• **Analyze organizational and operational environment** • **Apply systems security principles** • **Develop system requirements** • **Create system security architecture and design**
Exam Weight: 22%	**Exam Weight: 30%**
Domain 4: Secure Operations, Maintenance and Disposal	**Domain 4:** **Systems Implementation, Verification and Validation**
• Secure Operations • Secure Maintenance • Secure Disposal	• **Implement, integrate and deploy security solutions** • **Verify and validate security solutions**
Exam Weight: 21%	**Exam Weight: 14%**
Domain 5: Systems Engineering Technical Management	**Domain 5:** **Secure Operations, Change Management and Disposal**
• Acquisition Process • System Development Methodologies • Technical Management Processes	• **Develop secure operations strategy** • **Participate in secure operations** • **Participate in change management** • **Participate in the disposal process**
Exam Weight: 11%	**Exam Weight: 17%**

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 a list of supplementary references at www.isc2.org/certifications/References.

Examination Policies and Procedures

(ISC)² recommends that CISSP-ISSEP 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