CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

Domain Refresh

Effective Date: May 1, 2021

*Please note: The **CISSP 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 Domain Refresh

On May 1, 2021, the domains for the (ISC)² CISSP® credential exam will be refreshed.

The content of the CISSP will be refreshed to reflect the most pertinent issues that cybersecurity 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 (CPE) requirements encompass the topic areas relevant to the roles and responsibilities of today's practicing cybersecurity professional.

As a result of the content refresh, the subdomains have been updated to describe the topics accurately. The weights for two of the domains have also changed.

Domain Comparison

April 2018 – April 2021	Effective May 1, 2021
Domain 1: Security and Risk Management	**Domain 1: Security and Risk Management**
• Understand and apply concepts of confidentiality, integrity and availability • Evaluate and apply security governance principles • Determine compliance requirements • Understand legal and regulatory issues that pertain to information security in a global context • Understand, adhere to, and promote professional ethics • Develop, document, and implement security policy, standards, procedures, and guidelines • Identify, analyze, and prioritize Business Continuity (BC) requirements • Contribute to and enforce personnel security policies and procedures • Understand and apply risk management concepts • Understand and apply threat modeling concepts and methodologies • Apply risk-based management concepts to the supply chain • Establish and maintain a security awareness, education, and training program	• Understand, adhere to, and promote professional ethics • Understand and apply security concepts • Evaluate and apply security governance principles • Determine compliance and other requirements • Understand legal and regulatory issues that pertain to information security in a holistic context • Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards) • Develop, document, and implement security policy, standards, procedures, and guidelines • Identify, analyze, and prioritize Business Continuity (BC) requirements • Contribute to and enforce personnel security policies and procedures • Understand and apply risk management concepts • Understand and apply threat modeling concepts and methodologies • Apply Supply Chain Risk Management (SCRM) concepts • Establish and maintain a security awareness, education, and training program
Exam Weight: 15%	**Exam Weight: 15%**

April 2018 – April 2021	Effective May 1, 2021
Domain 2: Asset Security	**Domain 2:** **Asset Security**
• Identify and classify information and assets • Determine and maintain information and asset ownership • Protect privacy • Ensure appropriate asset retention • Determine data security controls • Establish information and asset handling requirements	• Identify and classify information and assets • Establish information and asset handling requirements • Provision resources securely • Manage data lifecycle • Ensure appropriate asset retention (e.g., Eng-of-Life (EOL), End-of-Support (EOS)) • Determine data security controls and compliance requirements
Exam Weight: 10%	**Exam Weight: 10%**

April 2018 – April 2021	Effective May 1, 2021
Domain 3: Security Architecture and Engineering	**Domain 3:** **Security Architecture and Engineering**
• Implement and manage engineering processes using secure design principles • Understand the fundamental concepts of security models • Select controls based upon systems security requirements • Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption) • Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements • Assess and mitigate vulnerabilities in web-based systems • Assess and mitigate vulnerabilities in mobile systems • Assess and mitigate vulnerabilities in embedded devices • Apply cryptography • Apply security principles to site and facility design • Implement site and facility security controls	• Research, implement and manage engineering processes using secure design principles • Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula) • Select controls based upon systems security requirements • Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption) • Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements • Select and determine cryptographic solutions • Understand methods of cryptanalytic attacks • Apply security principles to site and facility design • Design site and facility security controls
Exam Weight: 13%	**Exam Weight: 13%**

April 2018 – April 2021	Effective May 1, 2021
Domain 4: Communication and Network Security	**Domain 4:** **Communication and Network Security**
• Implement secure design principles in network architectures • Secure network components • Implement secure communication channels according to design	• Assess and implement secure design principles in network architectures • Secure network components • Implement secure communication channels according to design
Exam Weight: 14%	**Exam Weight: 13%**

April 2018 – April 2021	Effective May 1, 2021
Domain 5: Identity and Access Management (IAM)	**Domain 5:** **Identity and Access Management (IAM)**
• Control physical and logical access to assets • Manage identification and authentication of people, devices, and services • Integrate identity as a third-party service • Implement and manage authorization mechanisms • Manage the identity and access provisioning lifecycle	• Control physical and logical access to assets • Manage identification and authentication of people, devices, and services • Federated identity with a third-party service • Implement and manage authorization mechanisms • Manage the identity and access provisioning lifecycle • Implement authentication systems
Exam Weight: 13%	**Exam Weight: 13%**

April 2018 – April 2021	Effective May 1, 2021
Domain 6: Security Assessment and Testing	**Domain 6:** **Security Assessment and Testing**
• Design and validate assessment, test, and audit strategies • Conduct security control testing • Collect security process data (e.g., technical and administrative) • Analyze test output and generate report • Conduct or facilitate security audits	• Design and validate assessment, test, and audit strategies • Conduct security control testing • Collect security process data (e.g., technical and administrative) • Analyze test output and generate report • Conduct or facilitate security audits
Exam Weight: 12%	**Exam Weight: 12%**

Prior to September 15, 2020	Effective May 1, 2021
Domain 7: Security Operations	**Domain 7: Security Operations**
• Understand and support investigations • Understand requirements for investigation types • Conduct logging and monitoring activities • Securely provisioning resources • Understand and apply foundational security operations concepts • Apply resource protection techniques • Conduct incident management • Operate and maintain detective and preventative measures • Implement and support patch and vulnerability management • Understand and participate in change management processes • Implement recovery strategies • Implement Disaster Recovery (DR) processes • Test Disaster Recovery Plans (DRP) • Participate in Business Continuity (BC) planning and exercises • Implement and manage physical security • Address personnel safety and security concerns	• Understand and comply with investigations • Conduct logging and monitoring activities • Perform Configuration Management (CM) (e.g., provisioning, baselining, automation) • Apply foundational security operations concepts • Apply resource protection • Conduct incident management • Operate and maintain detective and preventative measures • Implement and support patch and vulnerability management • Understand and participate in change management processes • Implement recovery strategies • Implement Disaster Recovery (DR) processes • Test Disaster Recovery Plans (DRP) • Participate in Business Continuity (BC) planning and exercises • Implement and manage physical security • Address personnel safety and security concerns
Exam Weight: 13%	**Exam Weight: 13%**

Prior to September 15, 2020	Effective May 1, 2021
Domain 8: Software Development Security	**Domain 8:** **Software Development Security**
• Understand and integrate security in the Software Development Life Cycle (SDLC) • Identify and apply security controls in development environments • Assess the effectiveness of software security • Assess security impact of acquired software • Define and apply secure coding guidelines and standards	• Understand and integrate security in the Software Development Life Cycle (SDLC) • Identify and apply security controls in development environments • Assess the effectiveness of software security • Assess security impact of acquired software • Define and apply secure coding guidelines and standards
Exam Weight: 10%	**Exam Weight: 11%**

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 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