CISSP®

Certified Information Systems Security Professional

Certification Exam Outline

Effective Date: April 2018

(ISC)^{2}® INSPIRING A SAFE AND SECURE CYBER WORLD.

About CISSP

The Certified Information Systems Security Professional (CISSP) is the most globally recognized certification in the information security market. CISSP validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization.

The broad spectrum of topics included in the CISSP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following 8 domains:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Experience Requirements

Candidates must have a minimum of 5 years cumulative paid work experience in 2 or more of the 8 domains of the CISSP CBK. Earning a 4-year college degree or regional equivalent or an additional credential from the (ISC)² approved list will satisfy 1 year of the required experience. Education credit will only satisfy 1 year of experience.

A candidate that doesn't have the required experience to become a CISSP may become an Associate of (ISC)² by successfully passing the CISSP examination. The Associate of (ISC)² will then have 6 years to earn the 5 years required experience. You can learn more about CISSP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/CISSP/experience-requirements.

Accreditation

CISSP was the first credential in the field of information security to meet 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. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the CISSP. 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 CAT Examination Information

The CISSP exam uses Computerized Adaptive Testing (CAT) for all English exams. CISSP exams in all other languages are administered as linear, fixed-form exams. You can learn more about CISSP CAT at www.isc2.org/certificatons/CISSP-CAT.

Length of exam	3 hours
Number of questions	100 - 150
Question format	Multiple choice and advanced innovative questions
Passing grade	700 out of 1000 points
Exam language availability	English
Testing center	(ISC)^2 Authorized PPC and PVTC Select Pearson VUE Testing Centers

CISSP CAT Examination Weights

Domains	Average Weight
1. Security and Risk Management	15%
2. Asset Security	10%
3. Security Architecture and Engineering	13%
4. Communication and Network Security	14%
5. Identity and Access Management (IAM)	13%
6. Security Assessment and Testing	12%
7. Security Operations	13%
8. Software Development Security	10%
Total:	**100%**

CISSP Linear Examination Information

Length of exam	6 hours
Number of questions	250
Question format	Multiple choice and advanced innovative questions
Passing grade	700 out of 1000 points
Exam language availability	French, German, Brazilian Portuguese, Spanish, Japanese, Simplified Chinese, Korean
Testing center	(ISC)^2 Authorized PPC and PVTC Select Pearson VUE Testing Centers

CISSP Linear Examination Weights

Domains	Weight
1. Security and Risk Management	15%
2. Asset Security	10%
3. Security Architecture and Engineering	13%
4. Communication and Network Security	14%
5. Identity and Access Management (IAM)	13%
6. Security Assessment and Testing	12%
7. Security Operations	13%
8. Software Development Security	10%
Total:	**100%**

Domain 1:
Security and Risk Management

1.1 Understand and apply concepts of confidentiality, integrity and availability

1.2 Evaluate and apply security governance principles

- Alignment of security function to business strategy, goals, mission, and objectives
- Organizational processes (e.g., acquisitions, divestitures, governance committees)
- Organizational roles and responsibilities
- Security control frameworks
- Due care/due diligence

1.3 Determine compliance requirements

- Contractual, legal, industry standards, and regulatory requirements
- Privacy requirements

1.4 Understand legal and regulatory issues that pertain to information security in a global context

- Cyber crimes and data breaches
- Licensing and intellectual property requirements
- Import/export controls
- Trans-border data flow
- Privacy

1.5 Understand, adhere to, and promote professional ethics

- (ISC)² Code of Professional Ethics
- Organizational code of ethics

1.6 Develop, document, and implement security policy, standards, procedures, and guidelines

1.7 Identify, analyze, and prioritize Business Continuity (BC) requirements

- Develop and document scope and plan
- Business Impact Analysis (BIA)

1.8 Contribute to and enforce personnel security policies and procedures

- Candidate screening and hiring
- Employment agreements and policies
- Onboarding and termination processes
- Vendor, consultant, and contractor agreements and controls
- Compliance policy requirements
- Privacy policy requirements

1.9 Understand and apply risk management concepts

- Identify threats and vulnerabilities
- Risk assessment/analysis
- Risk response
- Countermeasure selection and implementation
- Applicable types of controls (e.g., preventive, detective, corrective)
- Security Control Assessment (SCA)
- Monitoring and measurement
- Asset valuation
- Reporting
- Continuous improvement
- Risk frameworks

1.10 Understand and apply threat modeling concepts and methodologies

- Threat modeling methodologies
- Threat modeling concepts

1.11 Apply risk-based management concepts to the supply chain

- Risks associated with hardware, software, and services
- Third-party assessment and monitoring
- Minimum security requirements
- Service-level requirements

1.12 Establish and maintain a security awareness, education, and training program

- Methods and techniques to present awareness and training
- Periodic content reviews
- Program effectiveness evaluation

Domain 2: Asset Security

2.1 Identify and classify information and assets

- » Data classification
- » Asset Classification

2.2 Determine and maintain information and asset ownership

2.3 Protect privacy

- » Data owners
- » Data processers
- » Data remanence
- » Collection limitation

2.4 Ensure appropriate asset retention

2.5 Determine data security controls

- » Understand data states
- » Scoping and tailoring
- » Standards selection
- » Data protection methods

2.6 Establish information and asset handling requirements

Domain 3:
Security Architecture and Engineering

3.1 Implement and manage engineering processes using secure design principles

3.2 Understand the fundamental concepts of security models

3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- Client-based systems
- Server-based systems
- Database systems
- Cryptographic systems
- Industrial Control Systems (ICS)
- Cloud-based systems
- Distributed systems
- Internet of Things (IoT)

3.6 Assess and mitigate vulnerabilities in web-based systems

3.7 Assess and mitigate vulnerabilities in mobile systems

3.8 Assess and mitigate vulnerabilities in embedded devices

3.9 Apply cryptography

- Cryptographic life cycle (e.g., key management, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves)
- Public Key Infrastructure (PKI)
- Key management practices
- Digital signatures
- Non-repudiation
- Integrity (e.g., hashing)
- Understand methods of cryptanalytic attacks
- Digital Rights Management (DRM)

3.10 Apply security principles to site and facility design

3.11 Implement site and facility security controls

- Wiring closets/intermediate distribution facilities
- Server rooms/data centers
- Media storage facilities
- Evidence storage
- Restricted and work area security
- Utilities and Heating, Ventilation, and Air Conditioning (HVAC)
- Environmental issues
- Fire prevention, detection, and suppression

Domain 4:
Communication and Network Security

4.1 Implement secure design principles in network architectures

- Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- Internet Protocol (IP) networking
- Implications of multilayer protocols
- Converged protocols
- Software-defined networks
- Wireless networks

4.2 Secure network components

- Operation of hardware
- Transmission media
- Network Access Control (NAC) devices
- Endpoint security
- Content-distribution networks

4.3 Implement secure communication channels according to design

- Voice
- Multimedia collaboration
- Remote access
- Data communications
- Virtualized networks

Domain 5:
Identity and Access Management (IAM)

5.1 Control physical and logical access to assets

- Information
- Systems
- Devices
- Facilities

5.2 Manage identification and authentication of people, devices, and services

- Identity management implementation
- Single/multi-factor authentication
- Accountability
- Session management
- Registration and proofing of identity
- Federated Identity Management (FIM)
- Credential management systems

5.3 Integrate identity as a third-party service

- On-premise
- Cloud
- Federated

5.4 Implement and manage authorization mechanisms

- Role Based Access Control (RBAC)
- Rule-based access control
- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Attribute Based Access Control (ABAC)

5.5 Manage the identity and access provisioning lifecycle

- User access review
- System account access review
- Provisioning and deprovisioning

Domain 6:
Security Assessment and Testing

6.1 Design and validate assessment, test, and audit strategies

- Internal
- External
- Third-party

6.2 Conduct security control testing

- Vulnerability assessment
- Penetration testing
- Log reviews
- Synthetic transactions
- Code review and testing
- Misuse case testing
- Test coverage analysis
- Interface testing

6.3 Collect security process data (e.g., technical and administrative)

- Account management
- Management review and approval
- Key performance and risk indicators
- Backup verification data
- Training and awareness
- Disaster Recovery (DR) and Business Continuity (BC)

6.4 Analyze test output and generate report

6.5 Conduct or facilitate security audits

- Internal
- External
- Third-party

Domain 7: Security Operations

7.1 Understand and support investigations

- Evidence collection and handling
- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics, and procedures

7.2 Understand requirements for investigation types

- Administrative
- Criminal
- Civil
- Regulatory
- Industry standards

7.3 Conduct logging and monitoring activities

- Intrusion detection and prevention
- Security Information and Event Management (SIEM)
- Continuous monitoring
- Egress monitoring

7.4 Securely provisioning resources

- Asset inventory
- Asset management
- Configuration management

7.5 Understand and apply foundational security operations concepts

- Need-to-know/least privileges
- Separation of duties and responsibilities
- Privileged account management
- Job rotation
- Information lifecycle
- Service Level Agreements (SLA)

7.6 Apply resource protection techniques

- Media management
- Hardware and software asset management

7.7 Conduct incident management

- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Lessons learned

7.8 Operate and maintain detective and preventative measures

- Firewalls
- Intrusion detection and prevention systems
- Whitelisting/blacklisting
- Third-party provided security services
- Sandboxing
- Honeypots/honeynets
- Anti-malware

7.9 Implement and support patch and vulnerability management

7.10 Understand and participate in change management processes

7.11 Implement recovery strategies

- Backup storage strategies
- Recovery site strategies
- Multiple processing sites
- System resilience, high availability, Quality of Service (QoS), and fault tolerance

7.12 Implement Disaster Recovery (DR) processes

- Response
- Personnel
- Communications
- Assessment
- Restoration
- Training and awareness

7.13 Test Disaster Recovery Plans (DRP)

- Read-through/tabletop
- Walkthrough
- Simulation
- Parallel
- Full interruption

7.14 Participate in Business Continuity (BC) planning and exercises

7.15 Implement and manage physical security

- Perimeter security controls
- Internal security controls

7.16 Address personnel safety and security concerns

- Travel
- Security training and awareness
- Emergency management
- Duress

Domain 8:
Software Development Security

8.1 Understand and integrate security in the Software Development Life Cycle (SDLC)

- Development methodologies
- Maturity models
- Operation and maintenance
- Change management
- Integrated product team

8.2 Identify and apply security controls in development environments

- Security of the software environments
- Configuration management as an aspect of secure coding
- Security of code repositories

8.3 Assess the effectiveness of software security

- Auditing and logging of changes
- Risk analysis and mitigation

8.4 Assess security impact of acquired software

8.5 Define and apply secure coding guidelines and standards

- Security weaknesses and vulnerabilities at the source-code level
- Security of application programming interfaces
- Secure coding practices

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 Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Americas
Tel: +1.866.331.ISC2 (4722)
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