CISSP®

Certified Information Systems Security Professional

Certification **Exam Outline**

Effective Date: April 2015

(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 Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Experience Requirements

Candidates must have a minimum of 5 years cumulative paid full-time 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.

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	16%
2. Asset Security	10%
3. Security Engineering	12%
4. Communications and Network Security	12%
5. Identity and Access Management	13%
6. Security Assessment and Testing	11%
7. Security Operations	16%
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, Visually impaired
Testing center	(ISC)^2 Authorized PPC and PVTC Select Pearson VUE Testing Centers

CISSP Linear Examination Weights

Domains	Weight
1. Security and Risk Management	16%
2. Asset Security	10%
3. Security Engineering	12%
4. Communications and Network Security	12%
5. Identity and Access Management	13%
6. Security Assessment and Testing	11%
7. Security Operations	16%
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 Apply security governance principles through:

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

1.3 Compliance

- Legislative and regulatory compliance
- Privacy requirements compliance

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

- Computer crimes
- Licensing and intellectual property (e.g., copyright, trademark, digital-rights management)
- Import/export controls
- Trans-border data flow
- Privacy
- Data breaches

1.5 Understand professional ethics

- Exercise (ISC)² Code of Professional Ethics
- Support organization's code of ethics

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

1.7 Understand business continuity requirements

- Develop and document project scope and plan
- Conduct business impact analysis

1.8 Contribute to personnel security policies

- Employment candidate screening (e.g., reference checks, education verification)
- Employment agreements and policies
- Employment termination processes
- Vendor, consultant, and contractor controls
- Compliance
- Privacy

1.9 Understand and apply risk management concepts

- Identify threats and vulnerabilities
- Risk assessment/analysis (qualitative, quantitative, hybrid)
- Risk assignment/acceptance (e.g., system authorization)
- Countermeasure selection
- Implementation
- Types of controls (preventive, detective, corrective, etc.)
- Control assessment
- Monitoring and measurement
- Asset valuation
- Reporting
- Continuous improvement
- Risk frameworks

1.10 Understand and apply threat modeling

- Identifying threats (e.g., adversaries, contractors, employees, trusted partners)
- Determining and diagramming potential attacks (e.g., social engineering, spoofing)
- Performing reduction analysis
- Technologies and processes to remediate threats (e.g., software architecture and operations)

1.11 Integrate security risk considerations into acquisition strategy and practice

- Hardware, software, and services
- Third-party assessment and monitoring (e.g., on-site assessment, document exchange and review, process/policy review)
- Minimum security requirements
- Service-level requirements

1.12 Establish and manage information security education, training, and awareness

- Appropriate levels of awareness, training, and education required within organization
- Periodic reviews for content relevancy

Domain 2: Asset Security

2.1 Classify information and supporting assets (e.g., sensitivity, criticality)

2.2 Determine and maintain ownership (e.g., data owners, system owners, business/mission owners)

2.3 Protect privacy

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

2.4 Ensure appropriate retention (e.g., media, hardware, personnel)

2.5 Determine data security controls (e.g., data at rest, data in transit)

- Baselines
- Scoping and tailoring
- Standards selection
- Cryptography

2.6 Establish handling requirements (markings, labels, storage, destruction of sensitive information)

Domain 3: Security Engineering

3.1 Implement and manage engineering processes using secure design principles

3.2 Understand the fundamental concepts of security models (e.g., Confidentiality, Integrity, and Multi-level Models)

3.3 Select controls and countermeasures based upon systems security evaluation models

3.4 Understand security capabilities of information systems (e.g., memory protection, virtualization, trusted platform module, interfaces, fault tolerance)

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

- Client-based (e.g., applets, local caches)
- Server-based (e.g., data flow control)
- Database security (e.g., inference, aggregation, data mining, data analytics, warehousing)
- Large-scale parallel data systems
- Distributed systems (e.g., cloud computing, grid computing, peer to peer)
- Cryptographic systems
- Industrial control systems (e.g., SCADA)

3.6 Assess and mitigate vulnerabilities in web-based systems (e.g., XML, OWASP)

3.7 Assess and mitigate vulnerabilities in mobile systems

3.8 Assess and mitigate vulnerabilities in embedded devices and cyber-physical systems (e.g., network-enabled devices, Internet of things (IoT))

3.9 Apply cryptography

- Cryptographic life cycle (e.g., cryptographic limitations, algorithm/protocol governance)
- Cryptographic types (e.g., symmetric, asymmetric, elliptic curves)
- Public Key Infrastructure (PKI)
- Key management practices
- Digital signatures
- Digital rights management
- Non-repudiation
- Integrity (hashing and salting)
- Methods of cryptanalytic attacks (e.g., brute force, cipher-text only, known plaintext)

3.10 Apply secure principles to site and facility design

3.11 Design and implement physical security

- Wiring closets
- Server rooms
- Media storage facilities
- Evidence storage
- Restricted and work area security (e.g., operations centers)
- Data center security
- Utilities and HVAC considerations
- Water issues (e.g., leakage, flooding)
- Fire prevention, detection and suppression

Domain 4: Communications and Network Security

4.1 Apply secure design principles to network architecture (e.g., IP & non-IP protocols, segmentation)

- OSI and TCP/IP models
- IP networking
- Implications of multilayer protocols (e.g., DNP3)
- Converged protocols (e.g., FCoE, MPLS, VoIP, iSCSI)
- Software-defined networks
- Wireless networks
- Cryptography used to maintain communication security

4.2 Secure network components

- Operation of hardware (e.g., modems, switches, routers, wireless access points, mobile devices)
- Transmission media (e.g., wired, wireless, fiber)
- Network access control devices (e.g., firewalls, proxies)
- Endpoint security
- Content-distribution networks
- Physical devices

4.3 Design and establish secure communication channels

- Voice
- Multimedia collaboration (e.g., remote meeting technology, instant messaging)
- Remote access (e.g., VPN, screen scraper, virtual application/desktop, telecommuting)
- Data communications (e.g., VLAN, TLS/SSL)
- Virtualized networks (e.g., SDN, virtual SAN, guest operating systems, port isolation)

4.4 Prevent or mitigate network attacks

Domain 5: Identity and Access Management

5.1 Control physical and logical access to assets

- Information
- Systems
- Devices
- Facilities

5.2 Manage identification and authentication of people and devices

- Identity management implementation (e.g., SSO, LDAP)
- Single/multi-factor authentication (e.g., factors, strength, errors)
- Accountability
- Session management (e.g., timeouts, screensavers)
- Registration and proofing of identity
- Federated identity management (e.g., SAML)
- Credential management systems

5.3 Integrate identity as a service (e.g., cloud identity)

5.4 Integrate third-party identity services (e.g., on-premise)

5.5 Implement and manage authorization mechanisms

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

5.6 Prevent or mitigate access control attacks

5.7 Manage the identity and access provisioning lifecycle (e.g., provisioning, review)

Domain 6: Security Assessment and Testing

6.1 Design and validate assessment and test strategies

6.2 Conduct security control testing

- Vulnerability assessment
- Penetration testing
- Log reviews
- Synthetic transactions
- Code review and testing (e.g., manual, dynamic, static, fuzz)
- Misuse case testing
- Test coverage analysis
- Interface testing (e.g., API, UI, physical)

6.3 Collect security process data (e.g., management and operational controls)

- Account management (e.g., escalation, revocation)
- Management review
- Key performance and risk indicators
- Backup verification data
- Training and awareness
- Disaster recovery and business continuity

6.4 Analyze and report test outputs (e.g., automated, manual)

6.5 Conduct or facilitate internal and third party audits

Domain 7: Security Operations

7.1 Understand and support investigations

- Evidence collection and handling (e.g., chain of custody, interviewing)
- Reporting and documenting
- Investigative techniques (e.g., root-cause analysis, incident handling)
- Digital forensics (e.g., media, network, software, and embedded devices)

7.2 Understand requirements for investigation types

- Operational
- Criminal
- Civil
- Regulatory
- Electronic discovery (eDiscovery)

7.3 Conduct logging and monitoring activities

- Intrusion detection and prevention
- Security information and event management
- Continuous monitoring
- Egress monitoring (e.g., data loss prevention, steganography, watermarking)

7.4 Secure the provisioning of resources

- Asset inventory (e.g., hardware, software)
- Configuration management
- Physical assets
- Virtual assets (e.g., software-defined network, virtual SAN, guest operating systems)
- Cloud assets (e.g., services, VMs, storage, networks)
- Applications (e.g., workloads or private clouds, web services, software as a service)

7.5 Understand and apply foundational security operations concepts

- Need-to-know/least privilege (e.g., entitlement, aggregation, transitive trust)
- Separation of duties and responsibilities
- Monitor special privileges (e.g., operators, administrators)
- Job rotation
- Information lifecycle
- Service-level agreements

7.6 Employ 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 preventative measures

- Firewalls
- Intrusion detection and prevention systems
- Whitelisting/Blacklisting
- Third-party security services
- Sandboxing
- Honeypots/Honeynets
- Anti-malware

7.9 Implement and support patch and vulnerability management

7.10 Participate in and understand change management processes (e.g., versioning, baselining, security impact analysis)

7.11 Implement recovery strategies

- Backup storage strategies (e.g., offsite storage, electronic vaulting, tape rotation)
- Recovery site strategies
- Multiple processing sites (e.g., operationally redundant systems)
- System resilience, high availability, quality of service, and fault tolerance

7.12 Implement disaster recovery processes

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

7.13 Test disaster recovery plans

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

7.14 Participate in business continuity planning and exercises

7.15 Implement and manage physical security

- Perimeter (e.g., access control and monitoring)
- Internal security (e.g., escort requirements/visitor control, keys and locks)

7.16 Participate in addressing personnel safety concerns (e.g., duress, travel, monitoring)

Domain 8: Software Development Security

8.1 Understand and apply security in the software development lifecycle

- Development methodologies (e.g., Agile, Waterfall)
- Maturity models
- Operation and maintenance
- Change management
- Integrated product team (e.g., DevOps)

8.2 Enforce security controls in development environments

- Security of the software environments
- Security weaknesses and vulnerabilities at the source-code level (e.g., buffer overflow, escalation of privilege, input/output validation)
- Configuration management as an aspect of secure coding
- Security of code repositories
- Security of application programming interfaces

8.3 Assess the effectiveness of software security

- Auditing and logging of changes
- Risk analysis and mitigation
- Acceptance testing

8.4 Assess security impact of acquired software

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: +1.727.785.0189
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