CISSP®

# Certified Information Systems Security Professional

## ISC2 Certification

# Certification **Exam Outline**

Effective Date: April 15, 2024

ISC2™

# 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 body of knowledge ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following eight 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 five years cumulative, full-time experience in two or more of the eight domains of the current CISSP Exam Outline. Earning a post-secondary degree (bachelors or masters) in computer science, information technology (IT) or related fields may satisfy up to one year of the required experience or an additional credential from the ISC2 approved list may satisfy up to one year of the required experience. Part-time work and internships may also count towards the experience requirement.

A candidate that doesn't have the required experience to become a CISSP may become an Associate of ISC2 by successfully passing the CISSP examination. The Associate of ISC2 will then have six years to earn the five 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)

ISC2 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, German, Spanish-Modern, Japanese, Simplified Chinese exams. You can learn more about CISSP CAT at www.isc2.org/certificatons/CISSP-CAT.

| | |
|---|---|
| **Length of exam** | 3 hours |
| **Number of items** | 125 - 150 |
| **Item format** | Multiple choice and advanced innovative items |
| **Passing grade** | 700 out of 1000 points |
| **Exam language availability** | Chinese, English, German, Japanese, Spanish |
| **Testing center** | ISC2 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 Architecture and Engineering | 13% |
| 4. Communication and Network Security | 13% |
| 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, adhere to, and promote professional ethics

- » ISC2 Code of Professional Ethics
- » Organizational code of ethics

## 1.2 Understand and apply security concepts

- » Confidentiality, integrity, and availability, authenticity, and nonrepudiation (5 Pillars of Information Security)

## 1.3 Evaluate and apply security governance principles

- » Alignment of the security function to business strategy, goals, mission, and objectives
- » Organizational processes (e.g., acquisitions, divestitures, governance committees)
- » Organizational roles and responsibilities
- » Security control frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry (PCI), Federal Risk and Authorization Management Program (FedRAMP))
- » Due care/due diligence

## 1.4 Understand legal, regulatory, and compliance issues that pertain to information security in a holistic context

- » Cybercrimes and data breaches
- » Licensing and Intellectual Property requirements
- » Import/export controls
- » Transborder data flow
- » Issues related to privacy (e.g., General Data Protection Regulation (GDPR), California Consumer Privacy Act, Personal Information Protection Law, Protection of Personal Information Act)
- » Contractual, legal, industry standards, and regulatory requirements

## 1.5 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

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

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

- Business impact analysis (BIA)
- External dependencies

## 1.8 Contribute to and enforce personnel security policies and procedures

- Candidate screening and hiring
- Employment agreements and policy driven requirements
- Onboarding, transfers, and termination processes
- Vendor, consultant, and contractor agreements and controls

## 1.9 Understand and apply risk management concepts

- Threat and vulnerability identification
- Risk analysis, assessment, and scope
- Risk response and treatment (e.g., cybersecurity insurance)
- Applicable types of controls (e.g., preventive, detection, corrective)
- Control assessments (e.g., security and privacy)
- Continuous monitoring and measurement
- Reporting (e.g., internal, external)
- Continuous improvement (e.g., risk maturity modeling)
- Risk frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry (PCI))

## 1.10 Understand and apply threat modeling concepts and methodologies

## 1.11 Apply supply chain risk management (SCRM) concepts

- Risks associated with the acquisition of products and services from suppliers and providers (e.g., product tampering, counterfeits, implants)
- Risk mitigations (e.g., third-party assessment and monitoring, minimum security requirements, service level requirements, silicon root of trust, physically unclonable function, software bill of materials)

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

- Methods and techniques to increase awareness and training (e.g., social engineering, phishing, security champions, gamification)
- Periodic content reviews to include emerging technologies and trends (e.g., cryptocurrency, artificial intelligence (AI), blockchain)
- Program effectiveness evaluation

# Domain 2: Asset Security

## 2.1 Identify and classify information and assets

- Data classification
- Asset Classification

## 2.2 Establish information and asset handling requirements

## 2.3 Provision information and assets securely

- Information and asset ownership
- Asset inventory (e.g., tangible, intangible)
- Asset management

## 2.4 Manage data lifecycle

- Data roles (i.e., owners, controllers, custodians, processors, users/subjects)
- Data collection
- Data location
- Data maintenance
- Data retention
- Data remanence
- Data destruction

## 2.5 Ensure appropriate asset retention (e.g., End of Life (EOL), End of Support)

## 2.6 Determine data security controls and compliance requirements

- Data states (e.g., in use, in transit, at rest)
- Scoping and tailoring
- Standards selection
- Data protection methods (e.g., Digital Rights Management (DRM), data loss prevention (DLP), cloud access security broker (CASB))

# Domain 3: Security Architecture and Engineering

## 3.1 Research, implement and manage engineering processes using secure design principles

- Threat modeling
- Least privilege
- Defense in depth
- Secure defaults
- Fail securely
- Segregation of Duties (SoD)
- Keep it simple and small
- Zero trust or trust but verify
- Privacy by design
- Shared responsibility
- Secure access service edge

## 3.2 Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)

## 3.3 Select controls based upon systems security requirements

## 3.4 Understand security capabilities of Information Systems (IS) (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 (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- Distributed systems
- Internet of Things (IoT)
- Microservices (e.g., application programming interface (API))
- Containerization
- Serverless
- Embedded systems
- High-Performance Computing systems
- Edge computing systems
- Virtualized systems

## 3.6 Select and determine cryptographic solutions

- Cryptographic life cycle (e.g., keys, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)
- Public key infrastructure (PKI) (e.g., quantum key distribution)
- Key management practices (e.g., rotation)
- Digital signatures and digital certificates (e.g., non-repudiation, integrity)

## 3.7 Understand methods of cryptanalytic attacks

- Brute force
- Ciphertext only
- Known plaintext
- Frequency analysis
- Chosen ciphertext
- Implementation attacks
- Side-channel
- Fault injection
- Timing
- Man-in-the-Middle (MITM)
- Pass the hash
- Kerberos exploitation
- Ransomware

## 3.8 Apply security principles to site and facility design

## 3.9 Design 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 (e.g., natural disasters, man-made)
- Fire prevention, detection, and suppression
- Power (e.g., redundant, backup)

## 3.10 Manage the information system lifecycle

- Stakeholders needs and requirements
- Requirements analysis
- Architectural design
- Development /implementation
- Integration
- Verification and validation
- Transition/deployment
- Operations and maintenance/sustainment
- Retirement/disposal

# Domain 4: Communication and Network Security

## 1îá ŋéêíĜ ā§sēþ§ }§ā£»Ö éþ£Ös£éĺ§ā £Ö Ö§ċĔÚþÌ [þsÃ£Ċ§sċēþ§ā

- ¶ Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- ¶ Internet Protocol (IP) version 4 and 6 (IPv6) (e.g., unicast, broadcast, multicast, anycast)
- ¶ Secure protocols (e.g., Internet Protocol Security (IPSec), Secure Shell (SSH), Secure Sockets Layer (SSL)/ Transport Layer Security (TLS))
- ¶ Implications of multilayer protocols
- ¶ Converged protocols (e.g., Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP), InfiniBand over Ethernet, Compute Express Link)
- ¶ Transport architecture (e.g., topology, data/control/management plane, cut-through/store-and-forward)
- ¶ Performance metrics (e.g., bandwidth, latency, jitter, throughput, signal-to-noise ratio)
- ¶ Traffic flows (e.g., north-south, east-west)
- ¶ Physical segmentation (e.g., in-band, out-of-band, air-gapped)
- ¶ Logical segmentation (e.g., virtual local area networks (VLANs), virtual private networks (VPNs), virtual routing and forwarding, virtual domain)
- ¶ Micro-segmentation (e.g., network overlays/encapsulation; distributed firewalls, routers, intrusion detection system (IDS)/intrusion prevention system (IPS), zero trust)
- ¶ Edge networks (e.g., ingress/egress, peering)
- ¶ Wireless networks (e.g., Bluetooth, Wi-Fi, Zigbee, satellite)
- ¶ Cellular/mobile networks (e.g., 4G, 5G)
- ¶ Content distribution networks (CDN)
- ¶ Software defined networks (SDN), (e.g., application programming interface (API), Software-Defined Wide-Area Network, network functions virtualization)
- ¶ Virtual Private Cloud (VPC)
- ¶ Monitoring and management (e.g., network observability, traffic flow/shaping, capacity management, fault detection and handling)

## 1îđ J§sēþ§ Ö§ċĔÚþÌ sÚÑéÚÖ§ÖĊā

- ¶ Operation of infrastructure (e.g., redundant power, warranty, support)
- ¶ Transmission media (e.g., physical security of media, signal propagation quality)
- ¶ Network Access Control (NAC) systems (e.g., physical, and virtual solutions)
- ¶ Endpoint security (e.g., host-based)

## 1îČ 3ÑéĺŠ§ÖĊ ā§sēþ§ sÚÑÑēÖ£s[ċ£ÚÖ sÃ[ÖÖ§Íā [ssÚþ}£Ö» ċÚ }§ā£»Ö

- ¶ Voice, video, and collaboration (e.g., conferencing, Zoom rooms)
- ¶ Remote access (e.g., network administrative functions)
- ¶ Data communications (e.g., backhaul networks, satellite)
- ¶ Third-party connectivity (e.g., telecom providers, hardware support)

# Domain 5: Identity and Access Management (IAM)

## 5.1 Control physical and logical access to assets

- Information
- Systems
- Devices
- Facilities
- Applications
- Services

## 5.2 Design identification and authentication strategy (e.g., people, devices, and services)

- Groups and Roles
- Authentication, Authorization and Accounting (AAA) (e.g., multi-factor authentication (MFA), password-less authentication)
- Session management
- Registration, proofing, and establishment of identity
- Federated Identity Management (FIM)
- Credential management systems (e.g., Password vault)
- Single sign-on (SSO)
- Just-In-Time

## 5.3 Federated identity with a third-party service

- On-premises
- Cloud
- Hybrid

## 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)
- Risk based access control
- Access policy enforcement (e.g., policy decision point, policy enforcement point)

## 5.5 Manage the identity and access provisioning lifecycle

- Account access review (e.g., user, system, service)
- Provisioning and deprovisioning (e.g., on /off boarding and transfers)
- Role definition and transition (e.g., people assigned to new roles)
- Privilege escalation (e.g., use of sudo, auditing its use)
- Service accounts management

## 5.6 Implement authentication systems

# Domain 6: Security Assessment and Testing

## 6.1 Design and validate assessment, test, and audit strategies

- Internal (e.g., within organization control)
- External (e.g., outside organization control)
- Third-party (e.g., outside of enterprise control)
- Location (e.g., on-premise, cloud, hybrid)

## 6.2 Conduct security control testing

- Vulnerability assessment
- Penetration testing (e.g., red, blue, and/or purple team exercises)
- Log reviews
- Synthetic transactions/benchmarks
- Code review and testing
- Misuse case testing
- Coverage analysis
- Interface testing (e.g., user interface, network interface, application programming interface (API))
- Breach attack simulations
- Compliance checks

## 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

- Remediation
- Exception handling
- Ethical disclosure

## 6.5 Conduct or facilitate security audits

- Internal (e.g., within organization control)
- External (e.g., outside organization control)
- Third-party (e.g., outside of enterprise control)
- Location (e.g., on-premises, cloud, hybrid)

# Domain 7: Security Operations

## 7.1 Understand and comply with investigations

- Evidence collection and handling
- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics, and procedures
- Artifacts (e.g., data, computer, network, mobile device)

## 7.2 Conduct logging and monitoring activities

- Intrusion detection and prevention (IDPS)
- Security information and event management (SIEM)
- Continuous monitoring and tuning
- Egress monitoring
- Log management
- Threat intelligence (e.g., threat feeds, threat hunting)
- User and Entity Behavior Analytics (UEBA)

## 7.3 Perform configuration management (CM) (e.g., provisioning, baselining, automation)

## 7.4 Apply foundational security operations concepts

- Need-to-know/least privilege
- Segregation of Duties (SoD) and responsibilities
- Privileged account management
- Job rotation
- Service-level agreements (SLA)

## 7.5 Apply resource protection

- Media management
- Media protection techniques
- Data at rest/data in transit

## 7.6 Conduct incident management

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

## 7.7 Operate and maintain detection and preventative measures

- Firewalls (e.g., next generation, web application, network)
- Intrusion detection systems (IDS) and intrusion prevention systems (IPS)
- Whitelisting/blacklisting
- Third-party provided security services
- Sandboxing
- Honeypots/honeynets
- Anti-malware
- Machine learning and artificial intelligence (AI) based tools

## 7.8 Implement and support patch and vulnerability management

## 7.9 Understand and participate in change management processes

## 7.10 Implement recovery strategies

- Backup storage strategies (e.g., cloud storage, onsite, offsite)
- Recovery site strategies (e.g., cold vs. hot, resource capacity agreements)
- Multiple processing sites
- System resilience, high availability (HA), Quality of Service (QoS), and fault tolerance

## 7.11 Implement disaster recovery (DR) processes

- Response
- Personnel
- Communications (e.g., methods)
- Assessment
- Restoration
- Training and awareness
- Lessons learned

## 7.12 Test disaster recovery plans (DRP)

- Read-through/tabletop
- Walkthrough
- Simulation
- Parallel
- Full interruption
- Communications (e.g., stakeholders, test status, regulators)

## 7.13 Participate in Business Continuity (BC) planning and exercises

## 7.14 Implement and manage physical security

- Perimeter security controls
- Internal security controls

## 7.15 Address personnel safety and security concerns

- Travel
- Security training and awareness (e.g., insider threat, social media impacts, two-factor authentication (2FA) fatigue)
- Emergency management
- Duress

# Domain 8: Software Development Security

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

- Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps, Scaled Agile Framework)
- Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))
- Operation and maintenance
- Change management
- Integrated Product Team

## 8.2 Identify and apply security controls in software development ecosystems

- Programming languages
- Libraries
- Tool sets
- Integrated Development Environment
- Runtime
- Continuous Integration and Continuous Delivery (CI/CD)
- Software configuration management (CM)
- Code repositories
- Application security testing (e.g., static application security testing (SAST), dynamic application security testing (DAST), software composition analysis, Interactive Application Security Test (IAST))

## 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

- Commercial-off-the-shelf (COTS)
- Open source
- Third-party
- Managed services (e.g., enterprise applications)
- Cloud services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

## 8.5 Define and apply secure coding guidelines and standards

- Security weaknesses and vulnerabilities at the source-code level
- Security of application programming interfaces (API)
- Secure coding practices
- Software-defined security

# 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

ISC2 recommends that 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 ISC2's legal policies, please contact the ISC2 Legal Department at legal@isc2.org.

## Any Questions?

Contact ISC2 Candidate Services in your region:

**Americas**
Tel: +1.866.331.ISC2 (4722), press 1
Email: membersupport@isc2.org

**Asia Pacific**
Tel: +(852) 5803-5662
Email: isc2asia@isc2.org

**Europe, Middle East and Africa**
Tel: +44 (0)203 960 7800
Email: info-emea@isc2.org

ISC2