CISSP: Certified Information Systems Security Professional

Exam Domains

The CISSP exam tests your competence in eight domains. Think of the domains as specific knowledge areas you need to know based on your experience and education.

The domains draw from a range of information security topics within the (ISC)² Common Body of Knowledge (CBK).

Here's a closer look at the CISSP domains and how they're weighted on the exam:

Domains	**Weight**
1. Security and Risk Management	16%
2. Asset Security	10%
3. Security Engineering	12%
4. Communication 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%**

Security and Risk Management

- Confidentiality, integrity and availability concepts
- Security governance principles
- Compliance
- Legal and regulatory issues
- Professional ethics
- Security policies, standards, procedures and guidelines

Asset Security

- Information and asset classification
- Ownership (e.g., data owners, system owners)
- Protect privacy
- Appropriate retention
- Data security controls
- Handling requirements (e.g., markings, labels, storage)

Security Engineering

- Engineering processes using secure design principles
- Fundamental concepts of security models
- Security evaluation models
- Security capabilities of information systems
- Security architectures, designs and solution elements vulnerabilities
- Web-based systems vulnerabilities

- Mobile systems vulnerabilities
- Embedded devices and cyber-physical systems vulnerabilities
- Cryptography
- Site and facility design secure principles
- Physical security

Communication and Network Security

- Secure network architecture design (e.g., IP & non-IP protocols, segmentation)
- Secure network components
- Secure communication channels
- Network attacks

Identity and Access Management

- Physical and logical assets control
- Identification and authentication of people and devices
- Identity as a service (e.g., cloud identity)
- Third-party identity services (e.g., on-premise)
- Access control attacks
- Identity and access provisioning lifecycle (e.g., provisioning review)

Security Assessment and Testing

- Assessment and test strategies
- Security process data (e.g., management and operational controls)
- Security control testing
- Test outputs (e.g., automated, manual)
- Security architecture vulnerabilities

Security Operations

- Investigations support and requirements
- Logging and monitoring activities
- Provisioning of resources
- Foundational security operations concepts
- Resource protection techniques
- Incident management
- Preventative measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery processes and plans
- Business continuity planning and exercises
- Physical security
- Personnel safety concerns

Software Development Security

- Security in the software development lifecycle
- Development environment security controls
- Software security effectiveness
- Acquired software security impact