The 8 CISSP domains explained

The CISSP® (Certified Information Systems Security Professional) qualification is one of the most respected certifications in the information security industry, demonstrating an advanced knowledge of cyber security.

We recently discussed the benefits of becoming a CISSP. Now, we turn our attention to the structure of the qualification itself and the domains within it.

(ISC)², which developed and maintains the CISSP qualification, updated the structure of the certificate in 2015, moving from ten domains to eight. We'll begin by listing the eight domains, and then go on to explain each one in more detail.

What are the 8 CISSP domains?

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communications and Network Security
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

1) Security and Risk Management

This is the largest domain in CISSP, providing a comprehensive overview of the things you need to know about information systems management. It covers:

- The confidentiality, integrity and availability of information;
- Security governance principles;
- Compliance requirements;
- Legal and regulatory issues relating to information security;
- IT policies and procedures; and
- Risk-based management concepts.

2) Asset Security

This domain addresses the physical requirements of information security. It covers:

- The classification and ownership of information and assets;
- Privacy;
- Retention periods;
- Data security controls; and
- Handling requirements.

3) Security Architecture and Engineering

This domain covers several important information security concepts, including:

- Engineering processes using secure design principles;
- Fundamental concepts of security models;
- Security capabilities of information systems;
- Assessing and mitigating vulnerabilities in systems;
- Cryptography; and
- Designing and implementing physical security.

4) Communications and Network Security

This domain covers the design and protection of an organisation's networks. This includes:

- Secure design principles for network architecture;
- Secure network components; and
- Secure communication channels.

5) Identity and Access Management

This domain helps information security professionals understand how to control the way users can access data. It covers:

- Physical and logical access to assets;
- Identification and authentication;
- Integrating identity as a service and third-party identity services;
- Authorisation mechanisms; and
- The identity and access provisioning lifecycle.

6) Security Assessment and Testing

This domain focuses on the design, performance and analysis of security testing. It includes:

- Designing and validating assessment and test strategies;
- Security control testing;
- Collecting security process data;
- Test outputs; and
- Internal and third-party security audits.

7) Security Operations

This domain addresses the way plans are put into action. It covers:

- Understanding and supporting investigations;
- Requirements for investigation types;
- Logging and monitoring activities;
- Securing the provision of resources;
- Foundational security operations concepts;
- Applying resource protection techniques;
- Incident management;
- Disaster recovery;
- Managing physical security; and
- Business continuity.

8) Software Development Security

This domain helps professionals to understand, apply and enforce software security. It covers:

- Security in the software development life cycle;
- Security controls in development environments;
- The effectiveness of software security; and
- Secure coding guidelines and standards.