Document Generated: 11/07/2026

Learning Style: On Demand

Technology: ISC2

Difficulty: Intermediate

Course Duration: 28 Weeks

ISC2 Certified Information Systems Security Professional (CISSP)



The Certified Information Systems Security Professional (CISSP) is the most globally recognized information security certification, validating both the technical expertise and leadership capabilities needed to protect and manage modern enterprise environments. This CISSP certification training provides the comprehensive knowledge required to design, engineer, and maintain an organization’s overall security protocols.

Through this CISSP instructor-led virtual classroom course, you'll gain the skills and confidence to prepare for the (ISC)² CISSP exam. Delivered through expert-led sessions, the course covers the full CISSP CBK (Common Body of Knowledge) 8 domains, ensuring relevance across all areas of cybersecurity, risk management, and information assurance.

This CISSP online course combines technical depth with managerial insight, equipping professionals to lead cybersecurity programs, implement secure architectures, and oversee enterprise defenses. Graduates often advance into roles such as Security Architect, Security Consultant, Cybersecurity Manager, or Chief Information Security Officer (CISO), with an average salary of **$126,000 per year.**

Course Objectives:

- Apply the fundamental concepts and methods related to the fields of information technology and security.
- Align the overall organizational operational goals with security functions and implementations.
- Determine how to protect assets of the organization as they go through their life cycle.
- Leverage the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.
- Apply the security design principles to select appropriate mitigations for vulnerabilities present in common information system types and architectures.
- Explain the importance of cryptography and the security services it can provide in today's digital and information age.
- Evaluate the physical security elements relative to information security needs.
- Evaluate the elements that comprise communication and network security relative to information security needs.
- Leverage the concepts and architecture that define the associated technology and implementation systems and protocols at Open Systems Interconnection (OSI) model layers 1–7 to meet information security needs.
- Determine the appropriate access control models to meet business security requirements.
- Apply the physical and logical access controls to meet information security needs.

- Differentiate between primary methods for designing and validating test and audit strategies that support information security requirements.
- Apply the appropriate security controls and countermeasures to optimize an organization's operational function and capacity.
- Assess the information systems risks to an organization's operational endeavors.
- Determine the appropriate controls to mitigate specific threats and vulnerabilities.
- Apply the information systems security concepts to mitigate the risk of software and systems vulnerabilities throughout the systems' life cycles.

Audience:

The CISSP is ideal for those working in roles such as:

- Security Consultant
- Security Analyst
- Security Manager
- Security Auditor
- Security Architect
- IT Director/Manager
- Director of Security
- Network Architect
- Security Systems Engineer
- Chief Information Security Officer

Prerequisites:

- 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

Course Outline:

- Domain 1: Security and Risk Management
- Domain 2: Asset Security
- Domain 3: Security Architecture and Engineering
- Domain 4: Communication and Network Security
- Domain 5: Identity and Access Management
- Domain 6: Security Assessment and Testing
- Domain 7: Security Operations
- Domain 8: Software Development Security