Document Generated: 11/07/2026

Learning Style: Virtual Classroom

Technology:

Difficulty: Intermediate

Course Duration: 5 Days

Next Course Date: December 14, 2026

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:

The CISSP exam is rigorous, covering eight security domains essential for the protection of information systems, corporations and national infrastructures. Understanding that security is an enterprise wide problem, these domains provide the candidate with a broad understanding of the technical, managerial and human factors that must coordinate effectively to keep information and systems secure. These domains include:

The Eight Domains of the CISSP CBK (Common Body of Knowledge)

- Security and Risk Management
- Asset Security
- Security Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

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 (IAM)

Domain 6. Security Assessment and Testing

Domain 7. Security Operations

Domain 8. Software Development Security

Credly Badge:



Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges