THE LEARNING CENTER
A TECHNICAL TRAINING INSTITUTION

CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

A CISSP is an information assurance professional who designs, engineers, implements, and runs an information security program that assures the security of a business environment. The CISSP exam covers critical topics in security, including cloud computing, mobile security, application development security, risk management, and more.

To be eligible for this exam, you must have five years of cumulative, paid, full-time work experience. A one-year experience waiver can be granted for a four-year college degree or an approved credential.

Our unique model follows a streamlined approach to workforce development and skills attainment

Assess: Assess each student to determine existing skill sets

Educate: Deliver goal-specific training utilizing all delivery modalities

Mentor: Expose students to instructors and mentors with front-line IT and cybersecurity experience

Certify: Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate: Validate student abilities through performance analytics and real-world exercises hosted on a cyber range

Exam Objectives CISSP (May 2021):

Security and Risk Management 15%
Confidentiality; Security Governance; Compliance; Regulatory Issues; Professional Ethics; Security Policies

Asset Security 10%
Information Classification; Ownership; Privacy; Retention; Data Security; Handling Requirements

Security Architecture & Engineering 13%
Secure Design; Security Models; Evaluation; Architectures; Vulnerabilities; Cryptography; Site/Facility Design; Physical Security

Communication & Network Security 13%
Secure Design; Secure Components; Communication Channels; Network Attacks

Identity and Access Management 13%
Asset Control; Identification & Authorization; Identity Services; Access Control Attacks; Access Lifecycle

Security Assessment and Testing 12%
Assessment Strategies; Security Processes; Security Control Testing; Test Outputs; Vulnerabilities

Security Operations 13%
Investigations; Logging; Provisioning; Security Concepts; Resource Protection; Incidence Management; Preventative Measures; Patching; Recovery Strategies; Disaster Recovery; Business Continuity; Physical Security; Personnel Safety

Software Development Security 11%
Development Security Controls; Software Security Effectiveness; Third-Party Software Security

Included

40 hours of instructor-led training sessions
Experiential lab modules
$(ISC)^2$ authorized textbook/class materials