THE LEARNING CENTER
A TECHNICAL TRAINING INSTITUTION

CISSP®

Certified Information Systems Security Professional

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.

$(ISC)^2$ CCSP is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

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 (2021):

Security and Risk Management	15%
Asset Security	10%
Security Architecture & Engineering	13%
Communication & Network Security	13%
Identity and Access Management	13%
Security Assessment and Testing	12%
Security Operations	13%
Software Development Security	11%

Course Outline:

Domain 1: Security and Risk Management - Confidentiality; Security Governance; Compliance; Regulatory Issues; Professional Ethics; Security Policies

Domain 2: Asset Security - Information Classification; Ownership; Privacy; Retention; Data Security; Handling Requirements

Domain 3: Security Architecture & Engineering - Secure Design; Security Models; Evaluation; Architectures; Vulnerabilities; Cryptography; Site/Facility Design; Physical Security

Domain 4: Communication & Network Security - Secure Design; Secure Components; Communication Channels; Network Attacks

Domain 5: Identity and Access Management - Asset Control; Identification & Authorization; Identity Services; Access Control Attacks; Access Lifecycle

Domain 6: Security Assessment and Testing - Assessment Strategies; Security Processes; Security Control Testing; Test Outputs; Vulnerabilities

Domain 7: Security Operations - Investigations; Logging; Provisioning; Security Concepts; Resource Protection; Incidence Management; Preventative Measures; Patching; Recovery Strategies; Disaster Recovery; Business Continuity; Physical Security; Personnel Safety

Domain 8: Software Development Security - 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