APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

ISC2 Certified Information Systems Security Professional (CISSP) Training

Award Winning Training · Applied Technology Academy

The Certified Information Systems Security Professional (CISSP) is the most globally recognized certification in the information security market. CISSP validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization. The broad spectrum of topics included in the CISSP Common Body of Knowledge (CBK®) ensure its relevancy across all disciplines in the field of information security.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Advanced	**5 Days**	**5 years: 2+ of the 8 domains**	**$140,230**	**No**

Course Overview

In-depth coverage of the eight domains required to pass the CISSP exam:

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

Course Outline

- **Lesson 1: Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulations, Business Continuity)**
  - Understand and Apply Concepts of Confidentiality, Integrity, and Availability
  - Apply Security Governance Principles
  - Compliance
  - Understand Legal and Regulatory Issues that Pertain to Information Security in a Global Context
  - Develop and Implement Documented Security Policy, Standards, Procedures, and Guidelines
  - Understand Business Continuity Requirements
  - Contribute to Personnel Security Policies
  - Understand and Apply Risk Management Concepts

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

  - Understand and Apply Threat Modeling
  - Integrate Security Risk Considerations into Acquisitions Strategy and Practice
  - Establish and Manage Security Education, Training, and Awareness
- **Lesson 2: Asset Security (Protecting Security of Assets)**
  - Classify Information and Supporting Assets
  - Determine and Maintain Ownership
  - Protect Privacy
  - Ensure Appropriate Retention
  - Determine Data Security Controls
  - Establish Handling Requirements
- **Lesson 3: Security Engineering (Engineering and Management of Security)**
  - Implement and Manage an Engineering Life Cycle Using Security Design Principles
  - Understand Fundamental Concepts of Security Models
  - Select Controls and Countermeasures Based Upon Information Systems Security Standards
  - Understand the Security Capabilities of Information Systems
  - Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements
  - Assess and Mitigate Vulnerabilities in Web-based Systems
  - Assess and Mitigate Vulnerabilities in Mobile Systems
  - Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber-Physical Systems
  - Apply Cryptography
  - Apply Secure Principles to Site and Facility Design
  - Design and Implement Facility Security
- **Lesson 4: Communications and Network Security (Designing and Protecting Network Security)**
  - Apply Secure Design Principles to Network Architecture
  - Securing Network Components
  - Design and Establish Secure Communication Channels
  - Prevent or Mitigate Network Attacks
- **Lesson 5: Identity and Access Management (Controlling Access and Managing Identity)**
  - Control Physical and Logical Access to Assets
  - Manage Identification and Authentication of People and Devices
  - Integrate Identity as a Service (IDaaS)
  - Integrate Third-Party Identity Services
  - Implement and Manage Authorization Mechanisms
  - Prevent or Mitigate Access Control Attacks
  - Manage the Identity and Access Provisioning Life Cycle
- **Lesson 6: Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)**

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

  - Design and Validate Assessment and Test Strategies
  - Conduct Security Control Testing
  - Collect Security Process Data
  - Conduct or Facilitate Internal and Third-Party Audits
- **Lesson 7: Security Operations (e.g., Foundational Concepts, Investigations, Incident Management, Disaster Recovery)**
  - Understand and Support Investigations
  - Understand Requirements for Investigation Types
  - Conduct Logging and Monitoring Activities
  - Secure the Provisioning of Resources through Configuration Management
  - Understand and Apply Foundational Security Operations Concepts
  - Employ Resource Protection Techniques
  - Conduct Incident Response
  - Operate and Maintain Preventative Measures
  - Implement and Support Patch and Vulnerability Management
  - Participate in and Understand Change Management Processes
  - Implement Recovery Strategies
  - Implement Disaster Recovery Processes
  - Test Disaster Recovery Plan
  - Participate in Business Continuity Planning
  - Implement and Manage Physical Security
  - Participate in Personnel Safety
- **Lesson 8: Software Development Security (Understanding, Applying, and Enforcing Software Security)**
  - Understand and Apply Security in the Software Development Life Cycle
  - Enforce Security Controls in the Development Environment
  - Assess the Effectiveness of Software Security
  - Assess Software Acquisition Security

Intended Audience

- Anyone whose position requires CISSP certification
- Individuals who want to advance within their current computer security careers or migrate to a related career

Prerequisites

Requirements:

CISSP candidates must meet specific requirements, as established by ISC2 — see: https://www.isc2.org/cissp/default.aspx

Those without the required experience can take the exam to become an Associate of ISC2 while working toward the experience needed for full certification

CISSPs are required by ISC2 to earn 120 Continuing Professional Education (CPE) credits every three years

To be successful in this course, you should have a minimum of five years of experience working in IT Infrastructure and Cybersecurity.

Follow-On Courses

- Certified Cloud Security Professional (CCSP)
- Systems Security Certified Practitioner (SSCP)

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.