



**Internet  
Institute USA**

**CISSP**

# Certified Information Systems Security Professional

---

The Certified Information Systems Security Professional (CISSP) certification, from the International Information Systems Security Certification Consortium ISC<sup>2</sup> is considered by some to be the single most important step for many security professionals. The CISSP credential is earned by passing a CISSP examination composed of 250 multiple choice questions.

The exam questions are based on what ISC<sup>2</sup> refers to as the *common body of knowledge* (CBK). With this metric, an accomplished and experienced security professional should have a foundation in all 10 areas of the CBK, which are:

- Security Management Practices
- Security Architecture and Models
- Access Control Systems & Methodology
- Application Development Security
- Operations Security
- Physical Security
- Cryptography
- Telecommunications, Network, & Internet Security
- Business Continuity Planning
- Law, Investigations, & Ethics

This 5-day course covers high-level issues in the administration of security policies. This is not a hands-on course: CISSP candidates are expected to know how to provision and implement technical aspects of security in their own domain.

---

To register or to check on class schedules, or for additional information, see our Web site at <http://iiusatech.com>, or send us email at [info@iiusatech.com](mailto:info@iiusatech.com).

- Instructor-led classroom sessions
- Course textbook/materials

---

<http://iiusatech.com>

# Course Outline

## Certified Information Systems Security Professional

### IIUSA-335 Certified Information Systems Security Professional (CISSP) (5 days)

**Prerequisites:** A CISSP student should possess Cisco Certified Network Associate (CCNA) certification or the equivalent knowledge (working knowledge of basic network security and a solid grasp of TCP/IP and fundamental networking concepts), be familiar with encryption technologies: DES, 3DES, RSA, hashing algorithms (MD5/SHA), and IPSec.

The sequence of topics is as follows:

#### **Part 1: Security Management Practices**

Security management entails the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines.

Management tools such as data classification and risk assessment/analysis are used to identify threats, classify assets, and to rate system vulnerabilities so that effective controls can be implemented.

#### **Part 2: Security Architecture and Models**

The Security Architecture and Models domain contains the concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment, networks, applications and those controls used to enforce various levels of availability, integrity, and confidentiality.

#### **Part 3: Access Control Systems and Methodology**

Access controls are a collection of mechanisms that work together to create a security architecture to protect the assets of the information system.

#### **Part 4: Application Development Security**

This domain addresses the important security concepts that apply to application software development. It outlines the environment where software is designed and developed and explains the critical role software plays in providing information system security.

#### **Part 5: Operations Security**

Operations Security is used to identify the controls over hardware, media, and the operators and administrators with access privileges to any of these resources. Audit and monitoring are the mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process.

#### **Part 6: Physical Security**

The physical security domain provides protection

techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources.

#### **Part 7: Cryptography**

The cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.

#### **Part 8: Telecommunications, Network, and Internet Security**

The telecommunications, network, and Internet security domain discusses the:

- Network Structures
- Transmission methods
- Transport formats
- Security measures used to provide availability, integrity, and confidentiality
- Authentication for transmissions over private and public communications networks and media.

#### **Part 9: Business Continuity Planning**

The Business Continuity Plan (BCP) domain addresses the preservation and recovery of business operations in the event of outages.

#### **Part 10: Law, Investigations, and Ethics**

The Law, Investigations, and Ethics domain addresses:

- Computer crime laws and regulations
- The measures and technologies used to investigate computer crime incidents

### **Internet Institute USA**

2200 North Central Avenue; Suite 103

Phoenix, AZ 85004

602-776-4545 (phone); 480-452-1688(fax)

<http://iisusatech.com> • [info@iisusatech.com](mailto:info@iisusatech.com)