

Enroll Certificates

Secure Network Traffic by Using Certificates

Renew Certificates

Revoke Certificates

Back Up Certificates and Private Keys

Restore Certificates and Private Keys

### **Lesson 9: Enforcing Organizational Security Policies**

Perform a Risk Assessment

Enforce Corporate Security Policy Compliance

Enforce Legal Compliance

Enforce Physical Security Compliance

Educate Users

Plan for Disaster Recovery

Conduct a Security Audit

### **Lesson 10: Monitoring the Security Infrastructure**

Scan for Vulnerabilities

Monitor for Security Anomalies

Set Up a Honeypot

### **Lesson 11: Managing Security Incidents**

Respond to Security Incidents

Evidence Administration

Recover From a Security Incident

## Security + Credentialing

**Number of questions:** 100

**Length of test:** 90 minutes

**Passing score:** 750 on a scale of 100-900

**Recommended experience:** CompTIA Network+ certification and two years of technical networking experience, with an emphasis on security.

**Languages:** English, Spanish, German, Japanese, Chinese

**Exam codes:** SY0-201, JK0-015

### **New Exam:**

CompTIA has released the exam objectives for CompTIA Security+ SY0-301, which is now in development. The new exam is scheduled to launch in May 2011

## Instructor Led Learning 10 days

**Overview:** This course addresses the 10 domains of CISSP. It offers a job-related approach to the security process, and provides basic skills required to prepare for CISSP certification.

**Breakdown:** This course addresses the 10 domains of CISSP in 8 days of training followed by one day of exam preparation and an exam on the 10<sup>th</sup> day.

**Who Should Attend:** This course is for experienced IT security-related practitioners pursuing CISSP training and certification. Students will validate their knowledge by meeting the necessary preparation requirements to qualify to sit for the CISSP certification exam.

**Objectives:** Upon successful completion of this course, students will be able to:

- analyze information systems access control.
- analyze security architecture and design.
- analyze network security systems and telecommunications.
- analyze information security management goals.
- analyze information security classification and program development.
- analyze risk management criteria and ethical codes of conduct.
- analyze application security.
- analyze cryptography characteristics and elements.
- analyze physical security.
- analyze operations security.
- apply business continuity and disaster recovery plans.
- identify legal issues, regulations, compliance standards, and investigation practices relating to information systems security.

Extra time is taken in this delivery to ensure key concepts are understood fully.

**Prerequisite(s) or equivalent knowledge:**  
Network+ Certification (Fourth Edition) 2009 Objectives  
Security+ Certification (2008 Objectives)

**Prerequisite Comments:**  
Students should have some experience with Information Security concepts and practices. To earn the CISSP® certification, 4 years of full-time Experience in information security or 3 years plus a B.S. degree is required.

### Lesson 1: Information Security and Risk Management

- Information Security Management
- Security Awareness Training and Education
- Risk Management
- Ethics

### Lesson 2: Access Control

- Definitions and Key Concepts
- Information Classification
- Access Control Categories and Types
- Access Control Threats
- Access to Systems/Data
- Access Control Technologies
- Assurance Mechanisms

### Lesson 3: Cryptography

- Key Concepts and Definitions
- History
- Encryption Systems
- Symmetric and Asymmetric Algorithms
- Message Integrity Controls
- Digital Signatures
- Management of Cryptographic Systems
- Threats and Attacks

### Lesson 4: Physical Security

- Definitions and Key Concepts
- Site Location
- Layered Defense Model
- Infrastructure Support Systems
- Equipment Protection

### Lesson 5: Security Architecture and Design

- Components and Principles
- System Security Techniques
- Hardware
- Software
- Security Models and Architecture Theory
- Security Evaluation Methods and Criteria