



# Certified Information Systems Security Professional

BUILDING TRAINING SOLUTIONS  
FOR THE IT WORLD

**Number of Days:** 5  
**Format:** Instructor-Led  
**Class Code:** CISSP

**Recommended Course Sequence**

Knowledge of prerequisites noted below.

*Course content is subject to change without notice.*

**Course Description:**

CISSP training is an advanced course designed to meet the high demands of the information security industry by preparing students for the Certified Information Systems Security Professional (CISSP) exam. This certification is managed by the internationally recognized and highly prestigious International Information Systems Security Certifications Consortium ISC.

The exam covers ISC's ten domains from the Common Body of Knowledge (CBK), encompassing the whole of information security. The exam consists of 250 multiple-choice questions. Candidates have up to 6 hours to complete the examination.

**Target Student:**

IT Managers, Compliance or Auditor staff, and anyone who would benefit from a broad look at IT Security best practices.

**Prerequisites:**

Anyone may attend this course, but those with experience in one or more of the ten domains will reap the greatest benefits.

**Delivery Method:**

Instructor led, group-paced, classroom-delivery learning model with structured hands-on activities.

**At Course Completion:**

Course materials reflect the latest information system security issues, concerns, and countermeasures.

- Discusses all ten domains of Common Body of Knowledge (CBK), helping to prepare for the CISSP exam.
- The CBK is the compilation and distillation of all information systems security material collected internationally of relevance to information system security professionals.
- Ensures information system security professionals have an opportunity to review the CBK in-depth, in preparation for the certification examination and to stay current on the ever-evolving domains within the information system security field.
- Presents a high-level review of the main topics
- Identifies specific areas students should study for exam preparation
- Provides an overview of the scope of the field

## Course Outline

<b>Lesson 1: Access Controls</b>
■ Threat Modeling

# Certified Information Systems Security Professional

---

<ul style="list-style-type: none"><li>■ Asset Valuation</li><li>■ Vulnerability Analysis</li><li>■ Access Aggregation</li><li>■ User Entitlement</li><li>■ Access Review &amp; Audit</li><li>■ Identity and Access Provisioning Lifecycle (e.g., Provisioning, Review, Revocation)</li></ul>
<b>Lesson 2: Telecommunications &amp; Network Security</b>
<ul style="list-style-type: none"><li>■ Understand secure network architecture and design (e.g., IP &amp; non-IP protocols, segmentation)</li><li>■ OSI and TCP/IP models</li><li>■ IP networking</li><li>■ Implications of multi-layer protocols</li><li>■ Hardware (e.g., modems, switches, routers, wireless access points)</li><li>■ Transmission media (e.g., wired, wireless, fiber)</li><li>■ Network access control devices (e.g., firewalls, proxies)</li><li>■ Establish secure communication channels (e.g., VPN, TLS/SSL, VLAN)</li><li>■ Voice (e.g., POTS, PBX, VoIP)</li><li>■ Remote access (e.g., screen scraper, virtual application/desktop, telecommuting)</li><li>■ Data Communications</li><li>■ Understand network attacks (e.g., DDoS, spoofing, session hijack)</li></ul>
<b>Lesson 3: Information Security Governance &amp; Risk Management</b>
<ul style="list-style-type: none"><li>■ Organizational processes (e.g., acquisitions, divestitures, governance committees)</li><li>■ Security roles and responsibilities</li><li>■ Manage third-party governance (e.g., on-site assessment, document exchange and review, process/policy review)</li><li>■ Risk assessment/analysis (qualitative, quantitative, hybrid)</li><li>■ Tangible and intangible asset valuation</li><li>■ Manage personnel security</li><li>■ Employment candidate screening (e.g., reference checks, education verification, background checks)</li><li>■ Manage the Security Function</li><li>■ Budget</li><li>■ Metrics</li></ul>
<b>Lesson 4: Software Development Security</b>
<ul style="list-style-type: none"><li>■ Understand and apply security in the software development life cycle</li><li>■ Development Life Cycle</li><li>■ Understand the environment and security controls</li><li>■ Security of the software environment</li><li>■ Security issues in source code (e.g., buffer overflow, escalation of privilege, backdoor)</li><li>■ Assess the effectiveness of software security</li></ul>

# Certified Information Systems Security Professional

---

<ul style="list-style-type: none"><li>■ Certification and accreditation (i.e., system authorization)</li></ul>
<b>Lesson 5: Cryptography</b>
<ul style="list-style-type: none"><li>■ Understand the cryptographic life cycle (e.g., cryptographic limitations, algorithm/protocol governance)</li><li>■ Brute Force (e.g., rainbow tables, specialized/scalable architecture, GPUs, CUDA)</li><li>■ Use cryptography to maintain network security</li><li>■ Use cryptography to maintain application security</li></ul>
<b>Lesson 6: Security Architecture &amp; Design</b>
<ul style="list-style-type: none"><li>■ Web-based (e.g., XML, SAML, OWASP)</li><li>■ Database security (e.g., inference, aggregation, data mining, warehousing)</li><li>■ Distributed systems (e.g., cloud computing, grid computing, peer to peer)</li></ul>
<b>Lesson 7: Operations Security</b>
<ul style="list-style-type: none"><li>■ Understand security operations concepts</li><li>■ Asset management (e.g., equipment life cycle, software licensing)</li><li>■ Remediation and review (e.g., root cause analysis)</li><li>■ Preventive measures against attacks (e.g., malicious code, zero-day exploit, denial of service)</li><li>■ Understand change and configuration management (e.g., versioning, baselining)</li><li>■ Understand system resilience and fault tolerance requirements</li></ul>
<b>Lesson 8: Business Continuity &amp; Disaster Recovery Planning</b>
<ul style="list-style-type: none"><li>■ Exercise, assess and maintain the plan (e.g., version control, distribution)</li><li>■ Personnel privacy and safety (e.g., duress, travel, monitoring)</li></ul>
<b>Lesson 9: Legal, Regulations, Investigations and Compliance</b>
<ul style="list-style-type: none"><li>■ Understand professional ethics</li><li>■ (ISC)2 Code of Professional Ethics</li><li>■ Support organization's code of ethics</li><li>■ Policy, roles and responsibilities (e.g., rules of engagement, authorization, scope)</li><li>■ Hardware/embedded device analysis</li><li>■ Ensure security in contractual agreements and procurement processes (e.g., cloud computing, outsourcing, vendor governance)</li></ul>
<b>Lesson 10: Physical (Environment) Security</b>
<ul style="list-style-type: none"><li>■ Understand site and facility design considerations</li><li>■ Support the implementation and operation of facilities security (e.g., technology, physical, and network convergence)</li><li>■ Personnel privacy and safety (e.g., duress, travel, monitoring)</li></ul>