ISC2

CISSP: Certified Information Systems Security Professional

In this 5-day, scenario-based course, you'll focus on computer security as an applied process across job roles and industries. This instructor has done the work in the real world, and explains the "hard stuff" in ways that are easy to understand - and there is a lot of "hard stuff" in this class! You'll build a solid base in preparation for achieving the Certified Information Systems Security Professional (CISSP) certification. This live class is available virtually with RemoteLive™ or locally at our Phoenix, AZ location.

$3,095.00

- 5 Days
- Experienced instructor explains the "hard stuff" in ways that are easy to understand
- Solid base to prepare for CISSP certification

Upcoming Dates

Jun 23 - Jun 27
Aug 25 - Aug 29
Oct 20 - Oct 24
Dec 15 - Dec 19

Course Description

Information security is part of every IT professional's job. Hackers are constantly trying to compromise your networks, steal sensitive data, and overwhelm your systems. Planning, implementing, enforcing, or even removing security are tasks we all do to keep users and systems safe. Performing these tasks properly and in alignment with industry best practices is critical to virtually every technology role, from decision maker to developer to operator.

This scenario-based course focuses on computer security as an applied process across job roles and industries. The course also helps to prepare students for achieving the Certified Information Systems Security Professional (CISSP) certification. CISSP is widely regarded as the most valuable vendor-neutral credential a computer security professional can hold. It is frequently identified as a prerequisite for security jobs across all industries including security design, implementation, maintenance, policy development, and management of secured systems, process/procedures, policies, applications and networks.

This course is primarily for Information Technology Security Professionals who want to advance their security certifications such as Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified Ethical Hacker (CEH), and related courses. This course also covers most of the knowledge required to prepare for the Systems Security Certified Practitioner (SSCP) certification exam.

Is this Course a CISSP Certification Bootcamp?

The CISSP certification requires 5 or more years of experience in a paid, full-time Information Security Management role. IF you already have that amount of experience and are pursuing this certification, you've probably already started studying and preparing. You might have already taken and failed the exam. And you wouldn't be in this class if you felt you were ready to take it and pass it already.

Throughout the week, I won't just be teaching you topics, I'll be helping you decide how prepared you already are and how much more work you'll need to do. At the end of the class you'll need to decide for yourself how ready you are and how much work you'll need to do. That's the only way to know when you should schedule your exam. It might be a week, a month, or a year. That's entirely up to you.

To be clear – this course is is not a CISSP Certification Bootcamp. The CISSP certification focuses on knowledge that is gained from real-

world experience, not from a classroom or a book. If you expect to attend this class and then ace the exam with no previous knowledge or experience, and without any other work, that's not going to happen. This is one of the toughest certifications in IT, and that's not because it's easy.

Course Outline

1.Access Control

- Security Principles and the Principle of Least
- Privilege
- Confidentiality
- Integrity
- Availability
- Identification, Authentication, Authorization, Access, and Accounting
- Authentication Techniques and Standards
- Access Control Models
- Access Control Methods and Implementations
- Access Control Accounting and Auditing

2. Information Security Governance and Risk Management

- Fundamental Principles of Security
- Confidentiality
- Integrity
- Availability
- Balancing the Security Principles
- Security vs. Usability vs. Cost
- Security Definitions
- Types of Security Controls
- Security Frameworks
- ISO/IEC 27001
- COSO
- COBIT
- Process Management
- Security Management
- Risk Management
- Risk Assessment and Analysis
- Asset Classification
- Data Classification
- Risk Mitigation Strategies
- Policies
- Standards
- Guidelines
- Baselines
- Procedures
- Executive Leadership in Risk Management
- Implementing Governance and Compliance Strategies

3. Security Architecture and Design

- Computer System Architecture
- Operating System Security Architecture
- Application Security Architecture
- System Security Models
- Security Architecture Evaluation and Certification

- Trusted Computer System Evaluation Criteria (TCSEC, or Orange Book)
- Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
- System Testing and Certification

4. Business Continuity and Disaster Recovery Planning

- Standards and Best Practices
- Planning for Incidents
- The Business Continuity Process
- Implementing A Disaster Recovery Plan

5. Cryptography

- Overview of Cryptography
- The History of Cryptography (Without Math)
- The Use of Cryptography (With Math)
- Symmetric Key (Shared Secret Key) Cryptography
- Diffie-Hellman Key Agreement
- Asymmetric Key (Public – Private Key) Cryptography
- Digital Signature (Hash) Cryptography
- Implementing All Types of Cryptography in Cryptosystems
- Public Key Infrastructure (PKI) and Certificates
- Encrypted VPN Tunnels
- Digitally Signed Documents and Email
- Encrypting Data At Rest and In Transit

6. Legal, Regulations, Investigations and Compliance

- The Complexity of Cybercrime
- Regions
- Laws
- Law Enforcement
- Privacy Laws
- Intellectual Privacy Laws
- Eavesdropping and Workplace Spying Laws
- Legal Liability and Security Compliance
- Conducting a Security Investigation
- Ethics of Information Security

7. Operations Security (formerly Security Operations)

- The Role of Operations in Information Security
- Personnel Management and Administration
- Planning System Security
- Implementing and Maintaining System Security
- Applying Controls
- System Hardening
- Trusted Recovery
- Configuration Management
- Change Control Process
- Change Control Documentation
- Change Control Compliance and Auditing
- Vulnerability Assessment
- Continuous Security Lifecycle

8. Physical (Environmental) Security

- The Importance of Physical Security in Information Security
- Planning Physical Security
- Identifying and Protecting Assets
- Internal Physical Security Threats and Controls
- Perimeter Physical Security Threats and Controls
- External Physical Security Threats and Controls

9. Software Development Security

- Security as a Part of Software Development
- System Development Lifecycle
- Secure Software Development Lifecycle
- Software Development Models
- Change Control and Update Management
- Cloud Computing
- Web and Mobile Applications
- Database Management and Security
- Malicious Software
- Viruses
- Trojan Horses
- Worms
- Rootkits
- Backdoors

10. Telecommunications and Network Security

- The Open Systems Interconnect Model
- TCP/IP Security
- IPv4 Security and Threats
- IPv6 Security and Threats
- Network Cabling Types and Security
- Considerations
- Network Devices
- Hubs
- Switches
- Routers
- Bridges
- Gateways
- Security Network Devices
- Firewalls and Content Filters
- Proxy Servers
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Firewalls
- WAN Security
- Dial-Up Network Security
- Virtual Private Network (VPN) Security
- Internet Protocol Security (IPSec)

Audience

This course is primarily designed for the IT professional whose role includes some information security tasks or responsibilities. Common

job titles for students include CISO, Director, Manager, Supervisor, Analyst, Information Architect, Program Manager, Lead, Information Security Officer, Security Specialist, and Auditor. The ideal student has some practical experience in the information security industry. Experienced information security professionals will also find value in this course to update their security skills, expand their knowledge of theoretical security, practice security exercises in areas that require a “safe” environment, and deepen exposure to areas outside their current role.

Prerequisites

Before taking this course, students should meet the minimum experience requirements for CISSP certification as defined by ISC(2).

What You Will Learn

After completing this course, you will have an understanding of:

- Security Architecture and Design
- Implementing Governance Compliance Strategies and Risk Management
- Security Access Control models, methods and implementations.
- Disaster Recovery Planning
- Cryptography Methodology
- Operations in Information Security
- Legal, Regulations, Investigations and Compliance in Security
- Vulnerability Assessment
- Continuous Security Lifecycle
- Physical and Software Development Security
- Network Security Considerations