301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

View Full Course Details including Latest Schedule Online

(ISC)²

CISSP Certification Training

This certification will help you climb the corporate ladder from field work into management positions; it could even position you to attain more prestigious job roles such as the CIO or CSO of an organization, which require CISSP certification.

Course Overview

Our 5-day, instructor-led CISSP (Certified Information Systems Security Professional)training and certification boot camp in Washington, DC Metro, Tysons Corner, VA, Columbia, MD or Live Online is targeted toward managers, engineers, auditors and security professionals seeking to better their skills and learn about the latest technologies. It covers ten domains:

1. Access control
2. Telecommunications & network security
3. Information security governance & risk management
4. Software development security
5. Cryptography
6. Security architecture & design
7. Operations security
8. Business continuity & disaster recovery planning
9. Legal, regulations, investigations & compliance
10. Physical (environmental) security

This course will fully prepare you for the CISSP® Certification exam.

You must have at least five combined years of professional experience in two or more of the previously listed domains. Additionally, you should be familiar with TCP/IP and the UNIX, Linux and Windows operating systems. Though not required, it is also recommended that you have the CompTIA® Security+ Certification.

PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Course Outline

Security Governance Through Principles and Policies

- Understand and apply concepts of confidentiality, integrity and availability
- Evaluate and apply security governance principles
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Understand and apply threat modeling concepts and methodologies
- Apply risk-based management concepts

Personnel Security and Risk Management Concepts

- Personnel security policies and procedures
- Security governance
- Understand and apply risk management concepts
- Establish and maintain a security awareness, education and training program
- Manage the security function

Business Continuity Planning

- Planning for business continuity
- Project scope and planning
- Business impact assessment
- Continuity planning
- Plan approval and implementation

Laws Regulations and Compliance

- Categories of laws
- Laws
- Compliance
- Contracting and procurement

Protecting Security of Assets

- Identify and classify assets
- Determining ownership

- Using security baselines

Cryptography and Symmetric Key Algorithms

- Historical milestones in cryptography
- Cryptographic basics
- Modern cryptography
- Symmetric cryptography
- Cryptographic lifecycle

PKI and Cryptogrpahic Applications

- Asymmetric cryptography
- Hash functions
- Digital signatures
- Public Key Infrastructure
- Asymmetric key management
- Applied cryptography
- Cryptographic attacks

Principles of Secrity Models, Design and Capabilities

- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models
- Select controls based on systems security requirements
- Understand security capabilities of information systems

Security Vulnerabilities, Threats, and Countermeasures

- Assess and mitigate security vulnerabilities
- Client-based systems
- Sever-based systems
- Database systems security
- Distributed systems and endpoint security
- Internet of Things
- Industrial control systems
- 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
- Essential security protection mechanisms

- Common architecture flaws and security issues

Physical Security Requirements

- Apply security principles to site and facility design
- Implement site and facility security controls
- Implement and manage physical security

Secure Network Architecture and Securing Network Components

- OSI model
- TCP/IP model
- Converged protocols
- Wireless networks
- Secure network components
- Cabling, wireless, topology, communications and transmission media technology

Secure Communications and Network Attacks

- Network and protocol security mechanisms
- Secure voice communications
- Multimedia collaboration
- Manage email security
- Remote access security management
- Virtual private network
- Virtualization
- Network address translation
- Switching technologies
- WAN technologies
- Miscellaneous security control characteristics
- Security boundaries
- Prevent or mitigate network attacks

Managing Identity and Authentication

- Controlling access to assets
- Comparing identification and authentication
- Implementing identity management
- Managing the identity and access provisioning lifecycle provisioning

Controlling and Monitoring Access

- Comparing access control models
- Understanding access control attacks

Security Assessment and Testing

- Building a security assessment and testing program
- Performing vulnerability assessments
- Testing your software
- Implementing security management processes

Managing Security Operations

- Applying security operations concepts
- Securely provisioning resources
- Managing configuration
- Managing change
- Managing patches and reducing vulnerabilities

Preventing and Responding to Incidents

- Managing incident response
- Implementing detective and preventative measures
- Logging, monitoring and auditing

Disaster Recovery Planning

- The nature of disaster
- Understand system resilience and fault tolerance
- Recovery strategy
- Recovery plan development
- Training, awareness and documentation
- Testing and maintenance

Investigations and Ethics

- Investigations
- Major categories of computer crime
- Ethics

Software Development Security

- Introducing systems development controls
- Establishing databases and data warehousing
- Storing data and information
- Understanding knowledge-based systems

Malicious Code and Application Attacks

- Malicious code
- Password attacks
- Application attacks
- Web application security
- Reconnaissance attacks
- Masquerading attacks

Exam Information

CISSP Certification Exam Details:

In order to take the CISSP certification exam, candidates must register with $(ISC)^2$.

CISSP Exam Details

- Number of Questions: 100-150
- Test Duration: 3 Hours
- Passing Score: 700 out of 1000 points
- Test Format: Multiple choice
- Test Delivery: $(ISC)^2$

CISSP Certification Measures a Candidate's Knowledge in Each of these 8 Domains:

1. Security and Risk Management

2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management (IAM)
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

CISSP Certification Training FAQs

What is a CISSP Certification salary?

According to payscale.com, a professional with a CISSP Certification earns an average of $110,000 annually.

What are the requirements for CISSP Certification?

Passing the CISSP Certification exam is not the only step to earning your CISSP credential. Aspiring candidates must also have a minimum of five years cumulative paid work experience in two or more of the eight domains of the CISSP CBK, complete the endorsement process, agree to (ISC)²'s Code of Ethics and pay your first AMF.

How many CPE credits are needed to renew the CISSP Certification?

Candidates must earn 120 Continuing Professional Education (CPE) credits every 3 years to maintain the CISSP credential.

Who should take the CISSP Certification Training course?

This course is intended for IT security professionals with multiple years of experience in roles such as IT Consultants, Managers, Security Policy Writers, Privacy Officers, Information Security Officers, Network Administrators, Security Device Administrators or Security Engineers.

PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

This **CISSP Certification Training** course includes:

- 5 days of instructor-led training
- 180 day exam prep kit includes :
  - 906 exam-like questions
  - Custom quizzes
  - Answer explanations
  - Exam simulation and practice modes
  - Performance tracker
  - 892 key concepts flashcards
  - Offline study kit
  - Suggested study plan
  - Discussion board
- (ISC)² CISSP Certification Training book
- Pre and post assessments
- CISSP onsite exam scheduling
- Certificate of completion for up to 40 CEUs/CPEs to be used toward renewing relevant certifications
- CISSP course retake guarantee
- CISSP certification satisfies DOD 8570 IAT Level III, IAM Level II and IASAE I & II
- CISSP classes scheduled monthly for live online and in-person delivery in Columbia, MD & Tysons Corner, VA
- CISSP classes can also be delivered onsite for groups of 5 or more students
- Eligible for MyCAA scholarship
- The CISSP certification course also follows NICE framework for a cybersecurity workforce
- Notepad, pen and highlighter
- Variety of bagels, fruits, doughnuts and cereal available at the start of class*

- Tea, coffee and soda available throughout the day*
- Freshly baked cookies every afternoon*

*denotes this benefit is only available at participating locations.