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

View Full Course Details including Latest Schedule Online

(ISC)²

CISSP (Certified Information Systems Security Professional)

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.

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

Course Overview

Official (ISC)²® Training Seminar for the Certified Information Systems Security Professional (CISSP®) provides a comprehensive review of the knowledge required to effectively design, engineer and manage the overall security posture of an organization. This training course will help students review and refresh their knowledge and identify areas they need to study for the CISSP exam. Content aligns with and comprehensively covers the eight domains of the (ISC)² CISSP Common Body of Knowledge (CBK®), ensuring relevancy across all disciplines in the field of cybersecurity.

Official courseware is developed by (ISC)² – creator of the CISSP CBK – to ensure your training is relevant and up-to-date. Our instructors are verified security experts who hold the CISSP and have completed intensive training to teach (ISC)² content.

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. Domains include:

Domain 1: Security and Risk Management

Domain 2: Asset Security

Domain 3: Security Architecture and Engineering

Domain 4: Communication and Network Security

Domain 5: Identity and Access Management (IAM)

Domain 6: Security Assessment and Testing

Domain 7: Security Operations

Domain 8: Software Development 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.

Schedule

DATE	LOCATION	
4/08/24 - 4/12/24 (5 days)	**Live Online** Open	Contact Us
5/20/24 - 5/24/24 (5 days)	**Live Online** Open	Contact Us
6/03/24 - 6/07/24 (5 days)	**Live Online** Open	Contact Us
7/22/24 - 7/26/24 (5 days)	**Live Online** Open	Contact Us
8/12/24 - 8/16/24 (5 days)	**Columbia, MD** Open	Contact Us
9/23/24 - 9/27/24 (5 days)	**Live Online** Open	Contact Us
10/28/24 - 11/01/24 (5 days)	**Live Online** Open	Contact Us

DATE	LOCATION	
12/09/24 - 12/13/24 (5 days)	Columbia, MD Open	Contact Us
1/27/25 - 1/31/25 (5 days)	Columbia, MD Open	Contact Us
1/27/25 - 1/31/25 (5 days)	Live Online Open	Contact Us
3/31/25 - 4/04/25 (5 days)	Columbia, MD Open	Contact Us
3/31/25 - 4/04/25 (5 days)	Live Online Open	Contact Us

Program Level

Advanced

Training Delivery Methods

Group Live

Duration

5 Days / 32 hours Training

CPE credits

26 NASBA CPE Credits

Field of Study

Information Technology

Advanced Prep

N/A

Course Registration

Candidates can choose to register for the course by via any of the below methods:

- Email: Sales@phoenixts.com
- Phone: 301-582-8200
- Website: www.phoenixts.com

Upon registration completion candidates are sent an automated course registration email that includes attachments with specific information on the class and location as well as pre-course study and test preparation material approved by the course vendor. The text of the email contains a registration confirmation as well as the location, date, time and contact person of the class.

Online enrolment closes three days before course start date.

On the first day of class, candidates are provided with instructions to register with the exam provider before the exam date.

Complaint Resolution Policy

To view our complete Complaint Resolution Policy policy please click here: Complaint Resolution Policy

Refunds and Cancellations

To view our complete Refund and Cancellation policy please click here: Refund and Cancellation Policy

Course Outline

Chapter 1: The Information Security Environment

- Justify an organizational code of ethics.
- Relate confidentiality, integrity, availability, non-repudiation, authenticity, privacy and safety to due care and due diligence.
- Relate information security governance to organizational business strategies, goals, missions, and objectives.
- Apply the concepts of cybercrime to data breaches and other information security compromises.
- Relate legal, contractual, and regulatory requirements for privacy and data protection to information security objectives.

Chapter 2: Information Asset Security

- Relate the IT asset management and data security lifecycle models to information security.
- Explain the use of information classification and categorization, as two separate but related processes.
- Describe the different data states and their information security considerations.
- Describe the different roles involved in the use of information, and the security considerations for these roles.
- Describe the different types and categories of information security controls and their use.
  Select data security standards to meet organizational compliance requirements.

Chapter 3: Identity and Access Management (IAM)

- Explain the identity lifecycle as it applies to human and nonhuman users.
- Compare and contrast access control models, mechanisms, and concepts.
- Explain the role of authentication, authorization, and accounting in achieving information security goals and objectives.
- Explain how IAM implementations must protect physical and logical assets.
- Describe the role of credentials and the identity store in IAM systems.

Chapter 4: Security Architecture and Engineering

- Describe the major components of security engineering standards.
- Explain major architectural models for information security.
- Explain the security capabilities implemented in hardware and firmware.
- Apply security principles to different information systems architectures and their environments.
- Determine the best application of cryptographic approaches to solving organizational information security needs.
- Manage the use of certificates and digital signatures to meet organizational information security needs.
- Discover the implications of the failure to use cryptographic techniques to protect the supply chain.
- Apply different cryptographic management solutions to meet the organizational information security needs.
- Verify cryptographic solutions are working and meeting the evolving threat of the real world.
- Describe defenses against common cryptographic attacks.
- Develop a management checklist to determine the organization’s cryptologic state of health and readiness.

Chapter 5: Communication and Network Security

- Describe the architectural characteristics, relevant technologies, protocols and security considerations of each of the layers in the OSI model.
- Explain the application of secure design practices in developing network infrastructure.
- Describe the evolution of methods to secure IP communications protocols.
- Explain the security implications of bound (cable and fiber) and unbound (wireless) network environments.
- Describe the evolution of, and security implications for, key network devices.
- Evaluate and contrast the security issues with voice communications in traditional and VoIP infrastructures.
- Describe and contrast the security considerations for key remote access technologies.
- Explain the security implications of software-defined networking (SDN) and network virtualization technologies.

Chapter 6: Software Development Security

- Recognize the many software elements that can put information systems security at risk.
- Identify and illustrate major causes of security weaknesses in source code.
- Illustrate major causes of security weaknesses in database and data warehouse systems.
- Explain the applicability of the OWASP framework to various web architectures.
- Select malware mitigation strategies appropriate to organizational information security needs.
- Contrast the ways that different software development methodologies, frameworks, and guidelines contribute to systems security.
- Explain the implementation of security controls for software development ecosystems.
- Choose an appropriate mix of security testing, assessment, controls, and management methods for different systems and applications environments.

Chapter 7: Security Assessment and Testing

- Describe the purpose, process, and objectives of formal and informal security assessment and testing.
- Apply professional and organizational ethics to security assessment and testing.
- Explain internal, external, and third-party assessment and testing.
- Explain management and governance issues related to planning and conducting security assessments.
- Explain the role of assessment in data-driven security decision-making.

Chapter 8: Security Operations

- Show how to efficiently and effectively gather and assess security data.
- Explain the security benefits of effective change management and change control.
- Develop incident response policies and plans.
- Link incident response to needs for security controls and their operational use.
- Relate security controls to improving and achieving required availability of information assets and systems.
- Understand the security and safety ramifications of various facilities, systems, and infrastructure characteristics.

Chapter 9: Putting It All Together

- Explain how governance frameworks and processes relate to the operational use of information security controls.
- Relate the process of conducting forensic investigations to information security operations.
- Relate business continuity and disaster recovery preparedness to information security operations.
- Explain how to use education, training, awareness, and engagement with all members of the organization as a way to strengthen and enforce information security processes.
- Show how to operationalize information systems and IT supply chain risk management.

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

Finance your CISSP Training!

We have partnered with Meritize to provide our students with financing options to fund your education. Check your loan options in minutes without impacting your credit score. Click here to apply



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 CISSP Online Training 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.

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

Phoenix TS is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints re-garding registered sponsors may be submitted to the National Registry of CPE Sponsors through its web site: www.nasbaregistry.org

Starting at **$3,629**

[redacted]

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

ATTENTION

For GSA pricing or Contractor quotes call
301-258-8200 – Option 2.

GSA

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
- ISC2 CISSP Certification Exam voucher
- One (1) year access to CISSP ExSim-Max*
  - hundreds of practice questions covering all concepts of CISSP
  - available on laptop, tablet and smartphone
  - study whenever and wherever
  - Simulates the level of difficulty, question types and item distribution
  - Contains well-written questions by subject matter experts
  - Includes comprehensive explanations with detailed references
  - Provides score reports to focus your study time
  - Gives you the tools you need to pass the exam

- (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 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**

**ExSim-Max CISSP Practice Exams are not available in all CISSP classes. Check with your account executive to see if your class qualifies.*

***denotes this benefit is only available at participating locations.*