

[View Full Course Details including Latest Schedule Online](#)

(ISC)²

SSCP (Systems Security Certified Practitioner)

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

Phoenix TS SSCP course ensures participants have the skills to become successful IT security professionals.

Our 5-day instructor-led SSCP – Systems Security and Certified Practitioner training course in Washington, DC Metro, Columbia, MD or Live Online will provides students with in instructor led lecture, activities and exam review. At the conclusion of this course, participants will be able to:

- Describe security and the alignment of asset management to risk management.
- Appraise risk management options and the use of access controls to protect assets.
- Examine the field of cryptography to secure information and communication.
- Build a security posture by securing software, data, and endpoints.
- Apply network and communications security to establish a secure networked environment.
- Evaluate cloud and wireless security.
- Prepare for incident detection and response.
- Implement appropriate measures that contribute to the maturation of risk management.

Schedule

DATE	LOCATION	
6/03/24 - 6/07/24 (5 days)	Live Online Open	Contact Us
8/12/24 - 8/16/24 (5 days)	Live Online Open	Contact Us

DATE

11/04/24 - 11/08/24 (5 days)

LOCATION

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: Introducing Security and Aligning Asset Management to Risk Management

- Classify information security and security concepts.
- Summarize components of the asset management lifecycle .
- Identify common risks and vulnerabilities.
- Provide examples of appropriate risk treatment.

Chapter 2: Understanding Risk Management Options and the Use of Access Controls to Protect Assets

- Provide examples of functional security controls and policies for identified scenarios.
- Classify various access control models.
- Identify components of the identity management lifecycle.
- Recognize access control and authentication methods.

Chapter 3: Cryptography

- Identify the fundamental concepts of cryptography driving requirements and benefits.



- Recognize symmetric encryption methods.
- Use asymmetric encryption methods.
- Examine Public-Key Infrastructure (PKI) systems and certificates.
- Summarize fundamental key management terms and concepts.
- Recognize how to implement secure protocols.
- Review methods of cryptanalytic attack.

Chapter 4: Securing Software, Data, and Endpoints

- Discuss software systems and application security.
- Recognize data security concepts and skills.
- Identify malicious code and countermeasures.
- Evaluate Mobile Device Management (MDM) and security issues with mobile and autonomous endpoints.
- Review attacks and countermeasures for virtual machines.

Chapter 5: Network and Communications Security

- Recognize layers of the OSI Model, their functions, and attacks present at each layer.
- Identify commonly used ports and protocols.
- Select appropriate countermeasures for various network attacks.
- Summarize best practices for establishing a secure networked environment.

Chapter 6: Cloud and Wireless Security

- Recall cloud security concepts and configurations.
- Recognize types of virtualization and cloud security considerations.
- Summarize the types of telecommunications and network access controls.

Chapter 7: Incident Detection and Response

- Review the steps for monitoring, incident detection, and data loss prevention using all source intelligence.
- Identify the elements of an incident response policy and members of the incident response team (IRT).
- Classify the SSCP's role in supporting forensic investigations.

Chapter 8: Maturing Risk Management

- Identify operational aspects of change management.

- Summarize physical security considerations.
- Design a security education and awareness strategy.
- Recognize common security assessment activities.
- Classify the components of a business continuity plan and disaster recovery plan.

Exam Details

SSCP Exam and Testing:

For the SSCP certification, a candidate is required to have a minimum of 1 year of cumulative paid full-time work experience in one or more of the 7 domains of the SSCP CBK. If you do not have the required experience, you may still sit for the exam and become an Associate of (ISC)2 until you have gained the required experience. **SSCP Exam Details**

- Number of Questions: 125
- Passing Score: 700 points out of 1000
- Test Duration: 3 Hours
- Test Format: Multiple choice
- Test Delivery: (ISC)²

SSCP Certification Measures a Candidate's Knowledge in Each of these 7 Domains:

1. Security Operations and Administration
2. Access Controls
3. Risk Identification, Monitoring, and Analysis
4. Incident Response and Recovery
5. Cryptography
6. Network and Communications Security
7. System and Application Security

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



PhoenixTS

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

(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 **\$2,149**

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.