Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow Enterprise Computing Solutions Ltd, Part 1st Floor, Suite 1D/1, Central House, Otley Road, Harrogate, HG3 1UG

Email: education.ecs.baltic@arrow.com
Phone: 0870 251 1000

SSCP - Systems Security Certified Practitioner

CODE:	LENGTH:	PRICE:
ISC_SSCP	40 Hours (5 days)	Request Price

Description

Official ISC2 CBK Training for the SSCP

Official ISC2® Training Seminar for the Systems Security Certified Practitioner (SSCP®) provides a comprehensive review of the knowledge required to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability. This training course will help students review and refresh their knowledge and identify areas they need to study for the SSCP exam. Content aligns with and comprehensively covers the seven domains of the ISC2 SSCP Common Body of Knowledge (CBK®).

Official courseware is developed by ISC2 – creator of the SSCP CBK – to ensure your training is relevant and up-to-date. Our instructors are verified security experts who hold the SSCP and have completed intensive training to teach ISC2 content.

Training features:

- Instruction from an ISC2 Authorized Instructor
- Official ISC2 Student Training Guide
- Interactive flash cards to reinforce learning
- 20 content-specific learning activities and 12 applied scenarios
- 61 content specific activities, including 6 case studies
- 8 end of chapter quizzes with answer explanation to assess comprehension
- 180 question post course assessment with answer explanation highlighting areas for further study

Course Domains

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

When you redeem your voucher, please check the course scheduling on ISC2's course booking site. This 5-day course can be delivered either on an 8-week basis: Tuesday - Thursday (2.5 hours a day) or delivered over 1-week (5 consecutive days).

Objectives

After completing this course, the student 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.

Audience

This training course is intended for practitioners who have at least one year of cumulative, paid work experience in one or more of the seven domains of the ISC2 SSCP CBK and are pursuing SSCP training and certification to acquire the credibility and mobility to advance within their current information security careers. The training seminar is ideal for those with technical skills and practical, hand-on security knowledge working in operational IT positions such as, but not limited to:

- Network Security Engineer
- Systems/Network Administrator
- Security Analyst
- Systems Engineer
- Security Consultant/Specialist
- Security Administrator
- Systems/Network Analyst
- Database Administrator

Programme

Domains/Modules/Chapters
This course covers the following chapters and learning objectives:

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.

Note: Throughout this course, exam domains may be covered in several chapters. Included in the course is a table indicating where the exam outline

Further Information

ACE Credit:
The Official ISC2 CBK Training Seminar for the SSCP has earned ACE CREDIT. Students who complete the course can apply for two hours of lower division credit at participating universities and
colleges.
Find out more at ACE.

Session Dates

On request. Please Contact Us

Additional Information

This training is also available as onsite training. Please contact us to find out more.