ISC2 SSCP

OUR LEARNING EXCLUSIVE

- Custom exam prep software and materials
- Exam delivery in the classroom, with a **98% success rate**
- Course-specific thinQtank® Learning publications to keep the learning engaging
- Extended hours of training, including immersive hands-on exercises
- **We do not teach the test.** We always deliver valuable hands-on experience
- All reading material and study guides sent to you when you register
- Every course taught by working security practitioners

TRAINING CAMP FORMAT

thinQtank® Learning delivers this course as an **instructor-led training camp**, with the exam sat in the classroom as part of the camp. Camps are scheduled by cohort rather than to a fixed calendar, and the balance of lecture and lab work is set to suit the group and the delivery method. Contact us for the schedule covering your dates.

PREREQUISITES

- Systems administration experience
- Working familiarity with TCP/IP
- A practical understanding of UNIX, Linux and Windows
- Intermediate-level network security knowledge

TARGET AUDIENCE

- Network security engineers, security administrators and analysts
- Systems engineers and administrators taking on security responsibility
- Security specialists and consultants
- Database administrators and network analysts whose work touches security controls

EXAM

ISC2 SSCP — Systems Security Certified Practitioner

Exam outline effective 15 September 2024. Passing score 700 on a scale of 1000. One year of paid work experience in one or more of the seven domains is required to certify — pass without it and you become an Associate of ISC2 while you earn it.

Seven domains: Security Concepts and Practices · Access Controls · Risk Identification, Monitoring and Analysis · Incident Response and Recovery · Cryptography · Network and Communication Security · Systems and Application Security

SSCP is accredited to **ISO/IEC 17024** by ANAB and is approved by the US Department of Defense under **directive 8140.03**.

COURSE OVERVIEW

thinQtank® Learning offers an industry-unique training camp in which students earn the **ISC2 SSCP** certification. As with all our ISC2 training experiences, the exam is delivered in the classroom.

SSCP is the practitioner-level ISC2 credential — the hands-on counterpart to CISSP. It is for the people who implement, monitor and administer the infrastructure that a security policy is written about: access controls, network and communications security, cryptography, systems and application hardening, and the incident response and recovery that follows when something gets through.

The practical difference from CISSP is the experience bar. SSCP asks for **one year** of paid work in one or more of the seven domains, not five — and you may sit the exam before you have it, becoming an Associate of ISC2 while you earn it. The **exam voucher is available** at $249 USD.

COURSE OBJECTIVES

Primary course objectives:

- Make the business case for information security and align controls to it
- Apply the security concepts and practices a practitioner is held to daily
- Run integrated risk management: identify, assess, treat and monitor
- Turn a risk decision into a control that is deployed and measured
- Secure communications and networks: segmentation, remote access, wireless
- Implement and administer identity and access control across the estate
- Apply cryptography correctly, and manage the keys behind it
- Harden hardware, endpoints, servers and virtualized systems
- Secure applications, data and cloud services
- Respond to and recover from incidents, and support forensic investigation
- Plan business continuity and disaster recovery, and test the plan
- Work the cross-domain problems where these areas meet

DELIVERY METHODS

- Instructor-led training
- Immersive live-online training
- On-site and custom delivery

WHAT YOU WILL BE ABLE TO DO

- Administer access, networks and systems to a written security policy
- Apply cryptography where it belongs, and manage the keys behind it
- Respond to an incident without destroying the evidence
- Plan continuity and recovery, and test the plan rather than file it

EXCLUSIVE LEARNING PACKAGE

- Hands-on security lab environment
- Cryptography and PKI workshop materials
- Incident response and forensics tabletop pack
- SSCP video course
- SSCP reading plan and review guide
- SSCP certification practice exam

COURSE MODULES

01 The Business Case for Decision Assurance and Information Security
- Topic A: Why the organization is spending this money
- Topic B: Decision assurance, and what security is actually protecting

02 Information Security Fundamentals
- Topic A: Core concepts, terminology and the practitioner's role
- Topic B: Security policy, standards and the chain from one to the other

03 Integrated Information Risk Management
- Topic A: Identifying and assessing risk
- Topic B: Treatment options and residual risk
- Topic C: Monitoring and reporting risk over time

04 Operationalizing Risk Mitigation
- Topic A: Turning a risk decision into a deployed control
- Topic B: Measuring whether the control is working

05 Communications and Network Security
- Topic A: Network architecture and segmentation
- Topic B: Traffic controls, remote access and wireless
- Topic C: Network attacks and the defenses that answer them

06 Identity and Access Control
- Topic A: Identification, authentication and authorization
- Topic B: Access control models and their trade-offs
- Topic C: Administering access without accumulating privilege

07 Cryptography
- Topic A: What to use, and where
- Topic B: Public key infrastructure and certificate handling
- Topic C: Key management, and what a failure of it costs

08 Hardware and Systems Security
- Topic A: Endpoint, server and mobile hardening
- Topic B: Virtualization and the host underneath it
- Topic C: Malware, and detecting what got in

09 Applications, Data and Cloud Security
- Topic A: Securing applications and the data they hold
- Topic B: Cloud service and deployment models
- Topic C: What changes when the workload is not yours

10 Incident Response and Recovery
- Topic A: Detection, escalation and containment
- Topic B: Forensic handling — investigating without destroying evidence
- Topic C: Recovery and the lessons that follow

11 Business Continuity via Information Security and People Power
- Topic A: Continuity and disaster recovery planning
- Topic B: Testing the plan rather than filing it
- Topic C: The people the plan depends on

12 Cross-Domain Challenges
- Topic A: Where the domains meet, which is where real incidents live
- Topic B: Working problems that no single domain answers