SSCP®

Systems Security
Certified Practitioner

Certification **Exam Outline**

Effective Date: April 2015

(ISC)²® INSPIRING A SAFE AND SECURE CYBER WORLD.

About SSCP

The Systems Security Certified Practitioner (SSCP) is the ideal certification for those with proven technical skills and practical, hands-on security knowledge in operational IT roles. It provides confirmation of a practitioner's ability to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability.

The broad spectrum of topics included in the SSCP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following 7 domains:

- Access Controls
- Security Operations and Administration
- Risk Identification, Monitoring, and Analysis
- Incident Response and Recovery
- Cryptography
- Network and Communications Security
- Systems and Application Security

Experience Requirements

Candidates must have a minimum of 1 year cumulative paid full-time work experience in 1 or more of the 7 domains of the SSCP CBK.

A candidate that doesn't have the required experience to become an SSCP may become an Associate of (ISC)² by successfully passing the SSCP examination. The Associate of (ISC)² will then have 2 years to earn the 1 year required experience.

Accreditation

SSCP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

(ISC)² has an obligation to its membership to maintain the relevancy of the SSCP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the SSCP. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing information security professionals.

SSCP Examination Information

Length of exam	3 hours
Number of questions	125
Question format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English, Japanese, and Brazilian Portuguese
Testing center	Pearson VUE Testing Center

SSCP Examination Weights

Domains	Weight
1. Access Controls	16%
2. Security Operations and Administration	17%
3. Risk Identification, Monitoring, and Analysis	12%
4. Incident Response and Recovery	13%
5. Cryptography	9%
6. Network and Communications Security	16%
7. Systems and Application Security	17%
Total:	**100%**

Domain 1: Access Controls

1.1 Implement Authentication Mechanisms

- Single/multifactor authentication
- Single sign-on
- Device authentication

1.2 Operate Internetwork Trust Architectures (e.g., extranet, third-party connections, federated access)

- One-way trust relationships
- Two-way trust relationships
- Transitive trust

1.3 Participate in the Identity-Management Lifecycle

- Authorization
- Proofing
- Provisioning
- Maintenance
- Entitlement

1.4 Implement Access Controls (e.g., subject-based, object-based)

- Mandatory
- Non-Discretionary
- Discretionary
- Role-based
- Attribute-based

Domain 2: Security Operations and Administration

2.1 Understand and Comply with Codes of Ethics

- (ISC)^2 Code of Ethics
- Organizational code of ethics

2.2 Understand Security Concepts

- Confidentiality
- Integrity
- Availability
- Accountability
- Privacy
- Non-repudiation
- Least privilege
- Separation of duties

2.3 Document and Operate Security Controls

- Deterrent controls
- Preventative controls
- Detective controls
- Corrective controls
- Compensating controls

2.4 Participate in Asset Management

- Lifecycle
- Hardware
- Software
- Data

2.5 Implement and Assess Compliance with Controls

- Technical controls
- Operational controls
- Managerial controls (e.g., security policies, baselines, standards, and procedures)

2.6 Participate in Change Management

- Implementation of Configuration Management Plan
- Security impact assessment
- System architecture/interoperability of systems
- Testing /implementing patches, fixes, and updates (e.g., operating system, applications, SDLC)

2.7 Participate in Security Awareness and Training

2.8 Participate in Physical Security Operations (e.g., security assessment, cameras, locks)

Domain 3:
Risk Identification, Monitoring, and Analysis

3.1 Understand the Risk Management Process

- Risk Visibility and Reporting (e.g., risk register, sharing threat intelligence)
- Risk management concepts (e.g., impacts, threats, vulnerabilities)
- Risk assessment
- Risk treatment (accept, transfer, mitigate, avoid)
- Audit findings

3.2 Perform Security Assessment Activities

- Participation in security testing and evaluation
- Interpretation and reporting of scanning and testing results

3.3 Operate and Maintain Monitoring Systems (e.g., continuous monitoring)

- Events of interest
- Logging
- Source systems

3.4 Analyze Monitoring Results

- Security analytics, metrics, and trends (e.g., baseline)
- Visualization
- Event data analysis (e.g., log, packet dump, machine data)
- Communicate findings

Domain 4:
Incident Response and Recovery

4.1 Participate in Incident Handling

- Discovery
- Escalation
- Reporting and feedback loops (lessons learned)
- Incident response
- Implementation of countermeasures

4.2 Understand and support forensic investigations (e.g., first responder, evidence handling, chain of custody, preservation of scene)

4.3 Understand and Support Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

- Emergency response plans and procedures (e.g., information system contingency plan)
- Interim or alternate processing strategies
- Restoration planning
- Backup and redundancy implementation
- Testing and drills

Domain 5: Cryptography

5.1 Understand and Apply Fundamental Concepts of Cryptography

- Hashing
- Salting
- Symmetric/asymmetric encryption
- Digital signatures
- Non-repudiation

5.2 Understand Requirements for Cryptography (e.g., data sensitivity, regulatory requirements, end-user training)

5.3 Understand and Support Secure Protocols (e.g., differences in implementation, appropriate use)

5.4 Operate and implement cryptographic systems

- Fundamental key management concepts (e.g., key rotation, key composition, cryptographic attacks)
- Public key infrastructure
- Administration and validation (e.g., key creation, exchange, revocation, escrow)
- Web of Trust (e.g., PGP)
- Implementation of secure protocols (e.g., IPSec, SSL/TLS, S/MIME)

Domain 6:
Network and Communications Security

6.1 Understand Security Issues Related to Networks

- OSI and TCP/IP models
- Network topographies and relationships (e.g., ring, star, bus, mesh, tree)
- Commonly used ports and protocols

6.2 Protect Telecommunications Technologies

- Converged communications
- Attacks and countermeasures

6.3 Control Network Access

- Access control and monitoring (e.g., NAC, remediation, quarantine, admission)
- Access control standards and protocols (e.g., IEEE 802.1X, Radius, TACACS)
- Remote access operation and configuration (e.g., thin client, SSL VPN, IPSec VPN, telework)
- Attacks and countermeasures

6.4 Manage LAN-based security

- Separation of data plane and control plane
- Segmentation (e.g., VLAN, ACLs)
- Secure device management

6.5 Operate and Configure Network-Based Security Devices

- Firewalls and proxies
- Network intrusion detection/prevention systems
- Routers and switches
- Traffic-shaping devices (e.g., WAN optimization)

6.6 Implement and Operate Wireless Technologies

- Transmission security (e.g., WPA, WPA2/802.11i, AES, TKIP)
- Wireless security devices (e.g., dedicated/integrated WIPS, WIDS)
- Attacks and countermeasures (e.g., management protocols)

Domain 7:
Systems and Application Security

7.1 Identify and Analyze Malicious Code and Activity

- Malicious code (e.g., malware)
- Malicious code countermeasures (e.g., scanners, anti-malware, code signing, sandboxing)
- Malicious activity (e.g., social engineering, insider threat, data theft, DDoS, spoofing, phishing, pharming, spam, Botnet)
- Malicious activity countermeasures (e.g., user awareness, system hardening, patching, sandboxing)

7.2 Implement and Operate Endpoint Device Security (e.g., virtualization, thin clients, thick clients, USB devices)

- HIDS
- Host-based firewalls
- Application white listing
- Endpoint encryption
- Trusted platform module
- Mobile device management (e.g., COPE, BYOD, telework)
- Secure browsing (e.g., sandbox)

7.3 Operate and Configure Cloud Security

- Operation models (e.g., public, private, hybrid)
- Service models (e.g., DNS, email, proxy, VPN)
- Virtualization (e.g., hypervisor)
- Legal and privacy concerns (e.g., surveillance, data ownership, jurisdiction, eDiscovery)
- Data storage and transmission (e.g., archiving, recovery, resilience)
- Third-party/outsourcing requirements (e.g., SLA, data portability, data destruction, auditing)

7.4 Secure Big Data Systems

- Application vulnerabilities
- Architecture or design vulnerabilities

7.5 Operate and Secure Virtual Environments

- Software-defined networking
- Hypervisor
- Virtual appliances
- Continuity and resilience
- Attacks and countermeasures
- Shared storage

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at www.isc2.org/sscp-cbk-references.

Examination Policies and Procedures

(ISC)² recommends that SSCP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at www.isc2.org/exam-policies-procedures.

Legal Info

For any questions related to (ISC)²'s legal policies, please contact the (ISC)² Legal Department at legal@isc2.org.

Any Questions?

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Americas
Tel: +1.727.785.0189
Email: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 28506951
Email: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0)203 300 1625
Email: info-emea@isc2.org