SSCP®

Systems Security Certified Practitioner

ISC2 Certification

Certification **Exam Outline**

Effective Date: November 2021

ISC2™

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 seven domains:

- Security Operations and Administration
- Access Controls
- 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 one year cumulative work experience in one or more of the seven domains of the SSCP CBK. A one year prerequisite pathway will be granted for candidates who received a degree (bachelors or masters) in a cybersecurity program.

A candidate that doesn't have the required experience to become an SSCP may become an Associate of ISC2 by successfully passing the SSCP examination. The Associate of ISC2 will then have two years to earn the one year required experience. You can learn more about SSCP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/SSCP/experience-requirements.

Accreditation

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

Job Task Analysis (JTA)

ISC2 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	4 hours
Number of items	150
Item format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English, Japanese, Chinese, Korean, German, Spanish
Testing center	Pearson VUE Testing Center

SSCP Examination Weights

Domains	Weight
1. Security Operations and Administration	16%
2. Access Controls	15%
3. Risk Identification, Monitoring and Analysis	15%
4. Incident Response and Recovery	14%
5. Cryptography	9%
6. Network and Communications Security	16%
7. Systems and Application Security	15%
Total:	**100%**

Domain 1:
Security Operations and Administration

1.1 Comply with codes of ethics

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

1.2 Understand security concepts

- Confidentiality
- Integrity
- Availability
- Accountability
- Privacy
- Non-repudiation
- Least privilege
- Segregation of duties (SoD)

1.3 Identify and implement security controls

- Technical controls (e.g., session timeout, password aging)
- Physical controls (e.g., mantraps, cameras, locks)
- Administrative controls (e.g., security policies, standards, procedures, baselines)
- Assessing compliance
- Periodic audit and review

1.4 Document and maintain functional security controls

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

1.5 Participate in asset management lifecycle (hardware, software and data)

- Process, planning, design and initiation
- Development/Acquisition
- Inventory and licensing
- Implementation/Assessment
- Operation/Maintenance
- Archiving and retention requirements
- Disposal and destruction

1.6 Participate in change management lifecycle

- Change management (e.g., roles, responsibilities, processes)
- Security impact analysis
- Configuration management (CM)

1.7 Participate in implementing security awareness and training (e.g., social engineering/ phishing)

1.8 Collaborate with physical security operations (e.g., data center assessment, badging)

Domain 2: Access Controls

2.1 Implement and maintain authentication methods

- Single/Multi-factor authentication (MFA)
- Single sign-on (SSO) (e.g., Active Directory Federation Services (ADFS), OpenID Connect)
- Device authentication
- Federated access (e.g., Open Authorization 2 (OAuth2), Security Assertion Markup Language (SAML))

2.2 Support internetwork trust architectures

- Trust relationships (e.g., 1-way, 2-way, transitive, zero)
- Internet, intranet and extranet
- Third-party connections

2.3 Participate in the identity management lifecycle

- Authorization
- Proofing
- Provisioning/De-provisioning
- Maintenance
- Entitlement
- Identity and access management (IAM) systems

2.4 Understand and apply access controls

- Mandatory
- Discretionary
- Role-based (e.g., attribute-, subject-, object-based)
- Rule-based

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/Indicators of Compromise (IOC), Common Vulnerability Scoring System (CVSS))
- Risk management concepts (e.g., impact assessments, threat modelling)
- Risk management frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST))
- Risk tolerance (e.g., appetite)
- Risk treatment (e.g., accept, transfer, mitigate, avoid, ignore)

3.2 Understand legal and regulatory concerns (e.g., jurisdiction, limitations, privacy)

3.3 Participate in security assessment and vulnerability management activities

- Security testing
- Risk review (e.g., internal, supplier, architecture)
- Vulnerability management lifecycle

3.4 Operate and monitor security platforms (e.g., continuous monitoring)

- Source systems (e.g., applications, security appliances, network devices and hosts)
- Events of interest (e.g., anomalies, intrusions, unauthorized changes, compliance monitoring)
- Log management
- Event aggregation and correlation

3.5 Analyze monitoring results

- Security baselines and anomalies
- Visualizations, metrics, and trends (e.g., notifications, dashboards, timelines)
- Event data analysis
- Document and communicate findings (e.g., escalation)

Domain 4:
Incident Response and Recovery

4.1 Support incident lifecycle (e.g., National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO))

- Preparation
- Detection, analysis and escalation
- Containment
- Eradication
- Recovery
- Lessons learned/Implementation of new countermeasure

4.2 Understand and support forensic investigations

- Legal (e.g., civil, criminal, administrative) and ethical principles
- Evidence handling (e.g., first responder, triage, chain of custody, preservation of scene)
- Reporting of analysis

4.3 Understand and support business continuity plan (BCP) and disaster recovery plan (DRP) activities

- Emergency response plans and procedures (e.g., information systems contingency, pandemic, natural disaster, crisis management)
- Interim or alternate processing strategies
- Restoration planning
- Backup and redundancy implementation
- Testing and drills

Domain 5: Cryptography

5.1 Understand reasons and requirements for cryptography

- Confidentiality
- Integrity and authenticity
- Data sensitivity (e.g., personally identifiable information (PII), intellectual property (IP), protected health information (PHI))
- Regulatory and industry best practice (e.g., Payment Card Industry Data Security Standards (PCI-DSS), International Organization for Standardization (ISO))

5.2 Apply cryptography concepts

- Hashing
- Salting
- Symmetric/Asymmetric encryption/Elliptic curve cryptography (ECC)
- Non-repudiation (e.g., digital signatures/certificates, Hash-based Message Authentication Code (HMAC), audit trails)
- Strength of encryption algorithms and keys (e.g., Advanced Encryption Standards (AES), Rivest-Shamir-Adleman (RSA), 256-, 512-, 1024-, 2048-bit keys)
- Cryptographic attacks, cryptanalysis, and countermeasures (e.g., quantum computing)

5.3 Understand and implement secure protocols

- Services and protocols (e.g., Internet Protocol Security (IPsec), Transport Layer Security (TLS), Secure/Multipurpose Internet Mail Extensions (S/MIME), DomainKeys Identified Mail (DKIM))
- Common use cases
- Limitations and vulnerabilities

5.4 Understand and support public key infrastructure (PKI) systems

- Fundamental key management concepts (e.g., storage, rotation, composition, generation, destruction, exchange, revocation, escrow)
- Web of Trust (WOT) (e.g., Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), blockchain)

Domain 6: Network and Communications Security

6.1 Understand and apply fundamental concepts of networking

- Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- Network topologies
- Network relationships (e.g., peer-to-peer (P2P), client server)
- Transmission media types (e.g., wired, wireless)
- Software-defined networking (SDN) (e.g., Software-Defined Wide Area Network (SD-WAN), network virtualization, automation)
- Commonly used ports and protocols

6.2 Understand network attacks (e.g., distributed denial of service (DDoS), man-in-the-middle (MITM), Domain Name System (DNS) poisoning) and countermeasures (e.g., content delivery networks (CDN))

6.3 Manage network access controls

- Network access controls, standards and protocols (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.1X, Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+))
- Remote access operation and configuration (e.g., thin client, virtual private network (VPN))

6.4 Manage network security

- Logical and physical placement of network devices (e.g., inline, passive, virtual)
- Segmentation (e.g., physical/logical, data/control plane, virtual local area network (VLAN), access control list (ACL), firewall zones, micro-segmentation)
- Secure device management

6.5 Operate and configure network-based security devices

- Firewalls and proxies (e.g., filtering methods, web application firewall (WAF))
- Intrusion detection systems (IDS) and intrusion prevention systems (IPS)
- Routers and switches
- Traffic-shaping devices (e.g., wide area network (WAN) optimization, load balancing)

6.6 Secure wireless communications

- Technologies (e.g., cellular network, Wi-Fi, Bluetooth, Near-Field Communication (NFC))
- Authentication and encryption protocols (e.g., Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Extensible Authentication Protocol (EAP))
- Internet of Things (IoT)

Domain 7: Systems and Application Security

7.1 Identify and analyze malicious code and activity

- Malware (e.g., rootkits, spyware, scareware, ransomware, trojans, virus, worms, trapdoors, backdoors, fileless
- Malware countermeasures (e.g., scanners, anti-malware, code signing)
- Malicious activity (e.g., insider threat, data theft, distributed denial of service (DDoS), botnet, zero-day exploits, web-based attacks, advanced persistent threat (APT))
- Malicious activity countermeasures (e.g., user awareness, system hardening, patching, isolation, data loss prevention (DLP))
- Social engineering (e.g., phishing, impersonation)
- Behavior analytics (e.g., machine learning, Artificial Intelligence (AI), data analytics)

7.2 Implement and operate endpoint device security

- Host-based intrusion prevention system (HIPS)
- Host-based firewalls
- Application whitelisting
- Endpoint encryption (e.g., whole disk encryption)
- Trusted Platform Module (TPM)
- Secure browsing
- Endpoint Detection and Response (EDR)

7.3 Administer Mobile Device Management (MDM)

- Provisioning techniques (e.g., corporate owned, personally enabled (COPE), Bring Your Own Device (BYOD))
- Containerization
- Encryption
- Mobile application management (MAM)

7.4 Understand and configure cloud security

- Deployment models (e.g., public, private, hybrid, community)
- Service models (e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS))
- Virtualization (e.g., hypervisor)
- Legal and regulatory concerns (e.g., privacy, surveillance, data ownership, jurisdiction, eDiscovery)
- Data storage, processing, and transmission (e.g., archiving, recovery, resilience)
- Third-party/outsourcing requirements (e.g., service-level agreement (SLA), data portability, data destruction, auditing)
- Shared responsibility model

7.5 Operate and maintain secure virtual environments

- Hypervisor
- Virtual appliances
- Containers
- 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/certifications/References.

Examination Policies and Procedures

ISC2 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/Register-for-Exam.

Legal Info

For any questions related to ISC2's legal policies, please contact the ISC2 Legal Department at legal@isc2.org.

Any Questions?

Contact ISC2 Candidate Services in your region:

Americas
Tel: +1-727-785-0189
Email: info@isc2.org

Asia-Pacific
Tel: +852-5803-5662
Email: isc2asia@isc2.org

Europe, Middle East and Africa
Tel: +44 (0)203-960-7800
Email: info-emea@isc2.org