SSCP®

# Systems Security Certified Practitioner

## ISC2 Certification

# Certification **Exam Outline**

Effective Date: September, 2024

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 body of knowledge ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following domains:

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

## Experience Requirements

Experience Required: Candidates must have a minimum of one-year full-time experience in one or more of the domains of the current SSCP outline. Earning a post-secondary degree (bachelor's or master's) in computer science, information technology (IT) or related fields may satisfy up to one year of the required experience. Part-time work and internships may also count towards the experience requirement.

## 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** | 3 hours |
| **Number of items** | 125 |
| **Item format** | Multiple choice |
| **Passing grade** | 700 out of 1000 points |
| **Exam availability** | English, Japanese, Spanish |
| **Testing center** | Pearson VUE Testing Center |

# SSCP Examination Weights

| Domains | Weight |
|---|---|
| 1. Security Concepts and Practices | 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 Concepts and Practices

## 1.1 Comply with codes of ethics

- ISC2 Code of Ethics
- Organizational code of ethics

## 1.2 Understand security concepts

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

## 1.3 Identify and implement security controls

- Technical controls (e.g., firewalls, intrusion detection systems (IDS), access control list (ACL))
- Physical controls (e.g., mantraps, cameras, locks)
- Administrative controls (e.g., security policies, standards, procedures, baselines)
- Assessing compliance requirements
- Periodic audit and review

## 1.4 Document and maintain functional security controls

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

## 1.5 Support and implement asset management lifecycle (i.e., hardware, software, and data)

- Process, planning, design and initiation
- Development /Acquisition (e.g., DevSecOps, testing)
- Inventory and licensing (e.g., open source, closed-source)
- Implementation/Assessment
- Operation/Maintenance/End of Life (EOL)
- Archival and retention requirements
- Disposal and destruction

## 1.6 Support and/or implement change management lifecycle

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

## 1.7 Support and/or implement security awareness and training (e.g., social engineering/ phishing/tabletop exercises/awareness communications)

## 1.8 Collaborate with physical security operations (e.g., data center/facility assessment, badging and visitor management, personal device restrictions)

# 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 (e.g., certificate, Media Access Control (MAC) address, Trusted Platform Module (TPM))
- Federated access (e.g., Open Authorization 2 (OAuth2), Security Assertion Markup Language (SAML))

## 2.2 Understand and support internetwork trust architectures

- Trust relationships (e.g., 1-way, 2-way, transitive, zero)
- Internet, intranet, extranet, and demilitarized zone (DMZ)
- Third-party connections (e.g., application programming interface (API), app extensions, middleware)

## 2.3 Support and/or implement the identity management lifecycle

- Authorization
- Proofing
- Provisioning/De-provisioning
- Monitoring, Reporting, and Maintenance (e.g., role changes, new security standards)
- Entitlement (e.g., inherited rights, resources)
- Identity and access management (IAM) systems

## 2.4 Understand and administer access controls

- Mandatory
- Discretionary
- Role-based (e.g., subject-based, object-based, Privileged Access Management (PAM))
- Rule-based
- Attribute-based

# Domain 3: Risk Identification, Monitoring and Analysis

## 3.1 Understand risk management

- Risk visibility and reporting (e.g., risk register, sharing threat intelligence, indicators of Compromise (IOC), Common Vulnerability Scoring System (CVSS), socialization, MITRE/ATT&CK model)
- Risk management concepts (e.g., impact assessments, threat modeling, scope)
- Risk management frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST))
- Risk tolerance (e.g., appetite, risk quantification)
- Risk treatment (e.g., accept, transfer, mitigate, avoid, ignore)

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

## 3.3 Perform security assessments and vulnerability management activities

- Risk management frameworks implementation
- Security testing
- Risk review (e.g., internal, supplier, architecture)
- Vulnerability management lifecycle (e.g., scanning, reporting, analysis, remediation)

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

- Source systems (e.g., applications, security appliances, network devices, hosts)
- Events of interest (e.g., errors, omissions, anomalies, unauthorized changes, compliance violations, policy failures)
- Log management (e.g., policy, integrity, preservation, architectures, configuration, aggregation, tuning)
- Security information and event management (SIEM) (e.g., real-time monitoring, analysis, tracking, audit)

## 3.5 Analyze monitoring results

- Security baselines and anomalies (e.g., correlation, noise reduction)
- 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 Understand and support incident response lifecycle (e.g., National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO))

- Preparation (e.g., defining roles, training programs)
- Detection, analysis, and escalation (e.g., incident communication, public relations)
- Containment
- Eradication
- Recovery (e.g., incident documentation)
- Post incident activities (e.g., lessons learned, new countermeasures, continuous improvement)

## 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
- Organization Security Policy Compliance

## 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 (e.g., Restore Time Objective (RTO), Restore Point Objectives (RPO), Maximum Tolerable Downtime (MTD))
- Backup and redundancy implementation
- Testing and drills (e.g., playbook, tabletop, disaster recovery exercises, scheduling)

# 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))
- Cryptography entropy (e.g., quantum cryptography, quantum key distribution)

## 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)
- Cryptographic attacks and cryptanalysis

## 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 (e.g., credit card processing, file transfer, web client, virtual private network (VPN), transmission of PII data)
- 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) cache poisoning)

- Countermeasures (e.g., content delivery networks (CDN), firewalls, network access controls, intrusion detection and prevention systems (IDPS))

## 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), virtual desktop infrastructure)

## 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 appliances and services

- Firewalls and proxies (e.g., filtering methods, web application firewall (WAF), cloud access security broker (CASB))
- Intrusion detection systems (IDS) and intrusion prevention systems (IPS)
- Routers and switches
- Traffic-shaping devices (e.g., wide area network (WAN) optimization, load balancing)
- Network Access Control (NAC)
- Data Loss Prevention (DLP)
- Unified Threat Management (UTM)

## 6.6 Secure wireless communications

- Technologies (e.g., cellular network, Wi-Fi, Bluetooth, Near-Field Communication (NFC))
- Authentication and encryption protocols (e.g., Wi-Fi Protected Access (WPA), Extensible Authentication Protocol (EAP), Wi-Fi Protected Access 2 (WPA2), Wi-Fi Protected Access 3 (WPA3))

## 6.7 Secure and monitor Internet of Things (IoT) (e.g., configuration, network isolation, firmware updates, End of Life (EOL) management)

# 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, app/code/operating system (OS)/mobile code vulnerabilities)
- Malware countermeasures (e.g., scanners, anti-malware, containment and remediation, software security)
- Types of 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/training, system hardening, patching, isolation, data loss prevention (DLP))
- Social engineering methods (e.g., SPAM email, phishing/smishing/vishing, impersonation, scarcity, whaling)
- 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 intrusion detection system (HIDS)
- Host-based firewalls
- Application whitelisting
- Endpoint encryption (e.g., full disk encryption)
- Trusted Platform Module (TPM) (e.g., hardware security module management)
- Secure browsing (e.g., digital certificates)
- Endpoint detection and response (EDR)

## 7.3 Endpoint detection and response (EDR)

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

## 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, Virtual Private Cloud (VPC))
- Legal and regulatory concerns (e.g., privacy, surveillance, data ownership, jurisdiction, eDiscovery, shadow information technology (IT))
- Third-party/Outsourcing requirements (e.g., service-level agreement (SLA), data portability/ privacy/destruction/auditing)
- Shared responsibility model
- Data storage, processing, and transmission (e.g., archiving, backup, recovery, resilience)

## 7.5 Operate and maintain secure virtual environments

- Hypervisor (i.e., Type 1 (e.g., bare metal), Type 2 (e.g., software))
- Virtual appliances
- Containers
- Continuity and resilience
- Storage management (e.g., data domain)
- Threats, attacks, and countermeasures (e.g., brute-force attack, virtual machine escape, threat hunting)

# Additional Examination Information

## Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the body of knowledge 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 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: +1.866.331.ISC2 (4722), press 1
Email: membersupport@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