SSCP®

Systems Security
Certified Practitioner

An (ISC)² Certification

Übersicht der
Zertifizierungsanforderungen

Gültig ab: November 2021

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

Über SSCP

Die Zertifizierung zum Systems Security Certified Practitioner (SSCP®) ist ideal für diejenigen, die über nachgewiesene technische Fachkenntnisse und praktisches, praxisbezogenes Sicherheitswissen in operativen IT-Funktionen verfügen. Sie bestätigt die Fähigkeit, IT-Infrastruktur in Übereinstimmung mit Informationssicherheitsrichtlinien und -verfahren zu implementieren, zu überwachen und zu verwalten, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten.

Das breite Themenspektrum, das im SSCP Common Body of Knowledge (CBK®) enthalten ist, gewährleistet die Relevanz für alle Bereiche auf dem Gebiet der Informationssicherheit. Interessierte Kandidaten verfügen über Erfahrungen in den folgenden sieben Themengebieten:

- Sicherheitsprozesse und Systemadministrierung
- Zugangskontrollen
- Identifizierung, Überwachung und Analyse von Risiken
- Reaktion auf IT-Sicherheitsvorfälle und deren Behebung
- Kryptographie
- Netzwerk- und Kommunikationssicherheit
- Sicherheit von Systemen und Anwendungssoftware

Erforderliche Berufserfahrung

Kandidaten müssen mindestens ein Jahr kumulative Berufserfahrung in einem oder mehreren der sieben Gebiete des SSCP CBK vorweisen können. Kandidaten mit einem Abschluss (Bachelor oder Master) in einem Informationssicherheitsstudiengang, wird die erforderliche einjährige Berufserfahrung angerechnet.

Ein Kandidat, der nicht über die erforderliche Erfahrung verfügt, kann ein Associate of (ISC)² werden, indem er die SSCP-Prüfung erfolgreich ablegt. Der Associate of (ISC)² hat dann zwei Jahre Zeit die erforderliche einjährige Erfahrung zu sammeln. Weitere Informationen zu den Anforderungen an die SSCP-Erfahrung und zur Anrechnung von Teilzeitarbeit und Praktika finden Sie unter www.isc2.org/Certifications/SSCP/experience-requirements.

Akkreditierung

Der SSCP erfüllt die strengen Anforderungen der ANSI/ISO/IEC-Norm 17024.

Analyse der Arbeitsaufgaben (JTA)

(ISC)² ist gegenüber seinen Mitgliedern verpflichtet, den Qualitätsstandard des SSCP aufrechtzuerhalten. Die in regelmäßigen Abständen durchgeführte Analyse der Arbeitsaufgaben (Job Task Analysis, JTA) ist ein methodischer und wichtiger Prozess zur Ermittlung der Aufgaben, die von Sicherheitsfachkräften ausgeführt werden, die in den vom SSCP definierten Berufen tätig sind. Die Ergebnisse der JTA werden zur Aktualisierung der Prüfung verwendet. Dieses Verfahren gewährleistet, dass die Kandidaten in jenen Themenbereichen geprüft werden, die für die Aufgaben und Verantwortlichkeiten heutiger Informationssicherheitsexperten relevant sind.

Informationen zur SSCP-Prüfung

Dauer der Prüfung	4 Stunden
Anzahl der Fragen	150
Fragenformat	Multiple-Choice
Punkte zum Bestehen	700 von 1000 Punkten
Prüfungsverfügbarkeit	Englisch, Japanisch, Chinesisch, Koreanisch, Deutsch und Spanisch
Prüfungszentrum	Pearson VUE-Prüfungszentrum

Gewichtung der SSCP-Themenbereiche

Bereich	Gewichtung
1. Sicherheitsprozesse und Systemadministrierung	16%
2. Zugangskontrollen	15%
3. Identifizierung, Überwachung und Analyse von Risiken	15%
4. Reaktion auf IT-Sicherheitsvorfälle und deren Behebung	14%
5. Kryptographie	9%
6. Netzwerk- und Kommunikationssicherheit	16%
7. Sicherheit von Systemen und Anwendungssoftware	15%
Insgesamt:	**100%**

Bereich 1:
Sicherheitsprozesse und Systemadministrierung

1.1 Einhaltung von Code of Ethics

» (ISC)² Code of Ethics
» Unternehmenseigener Ethik-Kodex

1.2 Verstehen von Sicherheitskonzepten

» Vertraulichkeit
» Integrität
» Verfügbarkeit
» Rechenschaftspflicht
» Datenschutz
» Nichtabstreitbarkeit
» Geringste Berechtigungen (Least Privilege)
» Aufgabentrennung (Segregation of Duties, SoD)

1.3 Identifizierung und Umsetzung von Sicherheitsmaßnahmen

» Technische Maßnahmen (z. B. Sitzungszeitüberschreitung, Passwortalterung)
» Physische Maßnahmen (z. B. Personenschleusen, Kameras, Schlösser)
» Organisatorische Maßnahmen (z. B. Sicherheitsrichtlinien, Standards, Verfahren, Baselines)
» Bewertung der Einhaltung von Vorgaben
» Regelmäßiges Audits und Überprüfungen

1.4 Dokumentation und Pflege funktionaler Sicherheitsmaßnahmen

» Abschreckende Maßnahmen
» Präventive Maßnahmen
» Erkennende Maßnahmen
» Korrektive Maßnahmen
» Kompensierende Maßnahmen

1.5 Mitwirkung am Asset-Management-Lebenszyklus (Hardware, Software und Daten)

- Organisation, Planung, Entwurf und Einführung eines Asset Managements
- Eigenentwicklung versus Kauf/Akquisition
- Inventarisierung und Lizenzierung
- Einführung/Bewertung
- Betrieb/Wartung
- Anforderungen an Archivierung und Aufbewahrung
- Entsorgung und Vernichtung

1.6 Mitwirkung am Change-Management-Lebenszyklus

- Change-Management (z. B. Rollen, Verantwortlichkeiten, Prozesse)
- Analyse der Auswirkungen auf die Sicherheit
- Konfigurationsmanagement

1.7 Mitwirkung an der Umsetzung von Security Awareness Maßnahmen und Schulungen (z. B. Social Engineering/Phishing)

1.8 Zusammenarbeit mit den für die physische Sicherheit zuständigen Bereichen (z. B. Bewertung von Rechenzentren, Ausweisverfahren)

Bereich 2: Zugangskontrollen

2.1 Implementierung und Betreuung von Authentifizierungsverfahren

» Single-/Multifaktor-Authentifizierung (MFA)
» Einmalige Anmeldung (Single Sign-On, SSO) (z. B. Active Directory Federation Services (ADFS), OpenID Connect)
» Geräteauthentifizierung
» Föderierter Zugriff (z. B. Open Authorization 2 (OAuth2), Security Assertion Markup Language (SAML))

2.2 Umsetzung vertrauenswürdiger Netzwerke

» Vertrauensbeziehungen (z. B. einseitig, zweiseitig, transitiv, replace with Zero-Trust)
» Internet, Intranet und Extranet
» Verbindungen zur Dritten

2.3 Teilnahme am Lebenszyklus des Identitätsmanagements

» Autorisierung
» Identitätsprüfung
» Bereitstellung/Aufhebung der Bereitstellung
» Pflege
» Berechtigung
» Identitäts- und Zugriffsverwaltungssysteme (Identity and Access Management, IAM)

2.4 Verstehen und Anwenden von Zugriffskontrollmodellen

» Zwingend erforderlich
» Diskret
» Rollenbasiert (z. B. attribut-, subjekt-, objektbezogen)
» Regelbasiert

Bereich 3:
Identifizierung, Überwachung und Analyse von Risiken

3.1 Verständnis des Risikomanagementprozesses

» Risikotransparenz und -berichterstattung (z. B. Risikoregister, Austausch von Bedrohungsdaten/ Indikatoren einer Kompromittierung (Indicators of Compromise, IOC), Allgemeines Bewertungssystem für Schwachstellen (Common Vulnerability Scoring System, CVSS))
» Risikomanagementkonzepte (z. B. Folgenabschätzungen, Bedrohungsmodellierung)
» Regelwerke für das Risikomanagement (z. B. Internationale Organisation für Normung (ISO), National Institute of Standards and Technology (NIST))
» Risikotoleranz (z. B. Risikobereitschaft)
» Risikobehandlung (z. B. akzeptieren, übertragen, abmildern, vermeiden, ignorieren)

3.2 Verständnis der rechtlichen und behördlichen Vorgaben (z. B. Rechtsprechung, Beschränkungen, Datenschutz)

3.3 Teilnahme an Maßnahmen zur Sicherheitsbewertung und zum Schwachstellenmanagement

» IT-Sicherheitstests
» Risikoüberprüfung (z. B. intern, Lieferanten, Architektur)
» Lebenszyklus des Schwachstellenmanagements

3.4 Betrieb und Überwachung von IT-Sicherheitssystemen (z. B. kontinuierliche Überwachung)

» Arten der unterschiedlichen Quellsysteme (z. B. Anwendungen, Sicherheitsanwendungen, Netzwerkgeräte und Hosts)
» Auffällige Ereignisse (z. B. Anomalien, Eindringversuche, nicht autorisierte Änderungen, Überwachung der Einhaltung von Vorschriften)
» Verwaltung der Logdaten
» Aggregation und Korrelation von Ereignissen

3.5 Analyse der Überwachungsergebnisse

» IT-Sicherheitsmindestanforderungen und Anomalien
» Darstellung, Metriken und Trends (z. B. Benachrichtigungen, Dashboards, zeitlicher Ablauf)
» Analyse von Logdaten
» Dokumentation und Kommunikation der Ergebnisse (z. B. Eskalation)

Bereich 4:
Reaktion auf IT-Sicherheitsvorfälle und deren Behebung

4.1 Unterstützung der Behandlung von IT-Sicherheitsvorfällen (z. B. Internationale Organisation für Normung (ISO), National Institute of Standards and Technology (NIST))

» Vorbereitung
» Erkennung, Analyse und Eskalation
» Eindämmung
» Beseitigung
» Wiederherstellung
» Gewonnene Erkenntnisse/Umsetzung neuer Gegenmaßnahme

4.2 Verständnis und Unterstützung für forensische Untersuchungen

» Rechtliche (z. B. zivil-, straf- und verwaltungsrechtliche) und ethische Grundsätze
» Umgang mit Beweismitteln (z. B. Ersteinsatzkräfte, Triage, Beweiskette, Sicherung des Tatorts)
» Berichterstattung der Untersuchungsergebnisse

4.3 Verstehen und Unterstützen von Maßnahmen im Rahmen von Business-Continuity-Plan (BCP) und Notfallwiederherstellungsplan (DRP)

» Notfallpläne und -verfahren (z. B. für Informationssysteme, Pandemien, Naturkatastrophen, Krisenmanagement)
» Temporäre bzw. alternative Vorgehensweisen
» Wiederherstellungsplanung
» Implementierung von Konzepten zur Datensicherung und Redundanz
» Tests und Prüfung der Maßnahmen

Bereich 5: Kryptographie

5.1 Verständnis der Gründe für und Anforderungen an die Kryptographie

- Vertraulichkeit
- Integrität und Authentizität
- Datensensibilität (z. B. personenbezogene Daten (Personally Identifiable Information, PII), geistiges Eigentum (Intellectual Property, IP), geschützte Gesundheitsdaten (Protected Health Information, PHI))
- Gesetzliche und branchenübliche Best Practices (z. B. Payment Card Industry Data Security Standards (PCI-DSS), Internationale Organisation für Normung (ISO))

5.2 Anwendung von Kryptographiekonzepten

- Hashing
- Salting
- Symmetrische/Asymmetrische Verschlüsselung/Kryptographie mit elliptischen Kurven (Elliptic Curve Cryptography, ECC)
- Nichtabstreitbarkeit (z. B. digitale Signaturen/Zertifikate, Hash-based Message Authentication Code (HMAC), Prüfpfade)
- Stärke der Verschlüsselungsalgorithmen und Schlüssel (z. B. Advanced Encryption Standards (AES), Rivest-Shamir-Adleman (RSA), 256-, 512-, 1024-, 2048-Bit-Schlüssel)
- Kryptographische Angriffe, Kryptoanalyse und Gegenmaßnahmen (z. B. Quantencomputer)

5.3 Verständnis und Implementierung von sicheren Protokollen

- Dienste und Protokolle (z. B. Internet Protocol Security (IPsec), Transport Layer Security (TLS), Secure/Multipurpose Internet Mail Extensions (S/MIME), DomainKeys Identified Mail (DKIM))
- Typische Anwendungsfälle
- Limitierungen und Schwächen

5.4 Verständnis und Unterstützung von Public-Key-Infrastruktur (PKI)-Systemen

- Grundlegende Konzepte der Schlüsselverwaltung (z. B. Speicherung, Rotation, Zusammensetzung, Erzeugung, Vernichtung, Austausch, Widerruf, Treuhändler)
- Web of Trust (WOT) (z. B. Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), Blockchain)

Bereich 6: Netzwerk- und Kommunikationssicherheit

6.1 Verständnis und Anwendung grundlegender Netzwerkkonzepte

- Open Systems Interconnection (OSI)- und Transmission Control Protocol/Internet Protocol (TCP/IP)-Modelle
- Netzwerktopologien
- Netzwerkbeziehungen (z. B. Peer-to-Peer (P2P), Client-Server)
- Art der Übertragungsmedien (z. B. kabelgebunden, drahtlos)
- Software-Defined Networking (SDN) (z. B. Software-Defined Wide Area Network (SD-WAN), Netzwerkvirtualisierung, Automatisierung)
- Häufig verwendete Ports und Protokolle

6.2 Verständnis von Netzwerkangriffen (z. B. Distributed Denial-of- Service (DDoS), Man-in-the-Middle (MITM), Domain Name System (DNS) Poisoning) und Gegenmaßnahmen (z. B Content Delivery Networks, CDN)

6.3 Verwaltung von Netzwerkzugangskontrollen

- Netzwerkzugangskontrollen, Standards und Protokolle (z. B. Institute of Electrical and Electronics Engineers (IEEE) 802.1X, Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+))
- Betrieb und Konfiguration des Fernzugriffs (z. B. Thin Client, virtuelles privates Netzwerk (VPN))

6.4 Verwaltung der Netzwerksicherheit

- Logische und physische Platzierung von Netzwerkgeräten (z. B. inline, passiv, virtuell)
- Segmentierung (z. B. physisch/logisch, Daten/Kontrollebene, virtuelles lokales Netz (VLAN), access control list (ACL), Firewall-Zonen, Mikrosegmentierung)
- Sichere Geräteverwaltung

6.5 Betrieb und Konfiguration von netzwerkbasierten Sicherheitsgeräten

- Firewalls und Proxys (z. B. Filtermethoden, Webanwendungs-Firewall (WAF))
- Angriffserkennungssystem (Intrusion Detection Systems, IDS) und Angriffsverhinderungssystem (Intrusion Prevention Systems, IPS)
- Router und Switches
- Geräte zur Verkehrsoptimierung (z. B. WAN-Optimierung, Lastausgleich)

6.6 Sichere Drahtloskommunikation

- Technologien (z. B. Mobilfunknetz, Wi-Fi, Bluetooth, Near-Field Communication (NFC))
- Authentifizierungs- und Verschlüsselungsprotokolle (z. B. Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Extensible Authentication Protocol (EAP))
- Internet der Dinge (Internet of Things, IoT)

Bereich 7: System- und Anwendungssicherheit

7.1 Identifizierung und Analyse von bösartigem Code und verdächtigen Aktivitäten

- Malware (z. B. Rootkits, Spyware, Scareware, Ransomware, Trojaner, Viren, Würmer, Trapdoors, Backdoors, dateilose Malware)
- Malware-Gegenmaßnahmen (z. B. Scanner, Anti-Malware, Code-Signierung)
- Böswillige Aktivitäten (z. B. Insider-Bedrohungen, Datendiebstahl, Distributed Denial- of-Service (DDoS), Botnetze, Zero-Day-Exploits, webbasierte Angriffe, fortgeschrittene, andauernde Bedrohung (APT))
- Maßnahmen zur Bekämpfung böswilliger Aktivitäten (z. B. Sensibilisierung der Benutzer, Systemhärtung, Patches, Isolierung, Verhinderung von Datenverlust (Data Loss Prevention, DLP))
- Social Engineering (z. B. Phishing, Vortäuschung einer Identität)
- Verhaltensanalyse (z. B. maschinelles Lernen, künstliche Intelligenz (KI), Datenanalyse)

7.2 Implementierung und Betrieb der Endgerätesicherheit

- Host-basiertes IPS (Host-based Intrusion Prevention System, HIPS)
- Host-basierte Firewalls
- Whitelisting von Anwendungen
- Endgeräteverschlüsselung (z. B. Festplattenverschlüsselung)
- Trusted Platform Module (TPM)
- Sicherheit beim Surfen im Internet
- Endpunkterkennung und -reaktion (Endpoint Detection and Response, EDR)

7.3 Verwalten von Mobile Device Management (MDM)

- Bereitstellungstechniken (z. B. firmeneigen, persönlich aktiviert (COPE), Bring Your Own Device (BYOD))
- Containerisierung
- Verschlüsselung
- Verwaltung mobiler Anwendungen (Mobile Application Management, MAM)

7.4 Verständnis und Konfiguration von Cloud- Sicherheit

- Bereitstellungsmodelle (z. B. öffentlich, privat, hybrid, geteilt)
- Servicemodelle (z. B. Infrastruktur als Service (IaaS), Plattform als Service (PaaS) und Software als Service (SaaS))
- Virtualisierung (z. B. Hypervisor)
- Rechtliche und regulatorische Belange (z. B. Datenschutz, Überwachung, Dateneigentum, Rechtsprechung, eDiscovery)
- Datenspeicherung, -verarbeitung und -übertragung (z. B. Archivierung, Wiederherstellung, Ausfallsicherheit)
- Anforderungen an Dritte/Outsourcing (z. B. Service- Level-Agreement (SLA), Datenübertragbarkeit, Datenvernichtung, Auditing)
- Modell der geteilten Verantwortung

7.5 Betrieb und Wartung sicherer virtueller Umgebungen

- Hypervisor
- Virtuelle Geräte
- Container
- Kontinuität und Resilienz
- Angriffe und Gegenmaßnahmen
- Gemeinsam genutzter Speicher

Zusätzliche Informationen zur Prüfung

Ergänzende Quellen

Kandidaten wird die Online-Recherche und Überprüfung weiterer Quellen zur Unterstützung dieses CBK im Rahmen der Zertifizierung dringend empfohlen.

Die gesamte Liste der ergänzenden Quellen finden Sie unter www.isc2.org/certifications/References.

Prüfungsrichtlinien und -verfahren

(ISC)² empfiehlt SSCP-Kandidaten sich mit den Prüfungsrichtlinien und -verfahren vor der Registrierung vertraut zu machen. Eine umfassende Auflistung dieser Vorgaben finden Sie unter www.isc2.org/Register-for-Exam.

Rechtliche Hinweise

Wenn Sie Fragen zu den rechtlichen Richtlinien von (ISC)² haben, wenden Sie sich bitte an die Rechtsabteilung von (ISC)² unter legal@isc2.org.

Noch Fragen?

(ISC)² Amerika
Tel.: +1.866.331.ISC2 (4722)
E-Mail: info@isc2.org

(ISC)² Asien-Pazifik Tel.: +(852) 5803 5662
E-Mail: isc2asia@isc2.org

(ISC)² Eurasien
Tel.: +44 (0) 203 960 7800
E-Mail: info-emea@isc2.org