SSCP-Systems Security Certified Practitioner - Certification Preperation

Duration: 5 Days **Course Code: GK1642**

Overview:

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

Please noteTo register for the new (ISC)2 exam, you will need a Pearson VUE exam voucher. This exam voucher is not included in the course price.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

The SSCP is ideal for IT administrators, managers, directors and network security professionals responsible for the hands-on operational security of their organization's critical assets, including those in the following positions: Network Security EngineerSystems AdministratorSecurity AnalystSystems EngineerSecurity Consultant/SpecialistSecurity AdministratorSystems/Network AnalystDatabase Administrator

Objectives:

- **After completing this course you should be able to:**
- Understand the different Access Control systems and how they should be implemented to protect the system and data using the different levels of confidentiality, integrity, and availability.
- Understand the processes necessary for working with management and information owners, custodians, and users so that proper data classifications are defined. This will ensure the proper handling of all hard copy and electronic information as it is applied by the Security Operations and Administration.
- The Risk Identification, Monitoring, and Analysis Domain identifies the how to identify, measure, and control losses associated with adverse events. You will review,analyze, select, and evaluate safeguards for mitigating risk.
- Identify how to handle Incident Response and Recovery using consistent, applies approaches including the use of the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) concepts in order to mitigate damages, recover business operations, and avoid critical business interruption; and emergency response and post-disaster recovery.
- Identify and differentiate key cryptographic concepts and how to apply them, implement secure protocols, key management concepts, key administration and validation, and Public Key Infrastructure as it applies to securing communications in the presence of third parties.
- Define and identify the Networks and Communications Security needed to secure network structure, data transmission methods, transport formats, and the security measures used to maintain integrity, availability, authentication, and confidentiality of the information being transmitted.
- The Systems and Application Security section identifies and defines technical and non-technical attacks and how an organization can protect itself from these attacks including the concepts in endpoint device security, cloud infrastructure security, securing big data systems, and securing virtual environments.

Prerequisites:

Nederlands:

Een jaar werkervaring in de Information Security, met minimaal één domein uit het SSCP-CBK.

==========

English:

One year working in the Information Security arena, covering at least one of the domains from the SSCP CBK.

- G005 - CompTIA Network+

Testing and Certification

- Length of exam 3 hours
- Number of items 125
- Item format Multiple choice
- Passing grade 700 out of 1000 points
- Language availability English, Japanese and Brazilian Portuguese
-
- Security Operations and Administration 16%
- Access Controls 15%
- Risk Identification, Monitoring and Analysis 15%
- Incident Response and Recovery 14%
- Cryptography 9%
- Network and Communications Security 16%
- Systems and Application Security 15%

Total100%

Content:

- (ISC)² Code of Ethics
- Organizational code of ethics1.2 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.j., 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 review1.4 Document and maintain functional security controls
- Deterrent controls
- Preventative controls
- Detective controls
- Corrective controls
- Compensating controls1.5 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 destruction1.6 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)

- 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 connections2.3 Participate in the identity management lifecycle
- Authorization

- Preparation
- Detection, analysis and escalation
- Containment
- Eradication
- Recovery
- Lessons learned/implementation of new countermeasure4.2 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 analysis4.3 Understand and support business continuity plan (BCP) and disaster recovery plan (DRP)
- Emergency response plans and procedures (e.g., information system contingency, pandemic, natural disaster, crisis management)
- Interim or alternate processing strategies
- Restoration planning
- Backup and redundancy implementation
- Testing and drills

- 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
- Common use cases
- Limitations and vulnerabilities5.4 Understand public key infrastructure (PKI)
- Fundamental key management concepts (e.g., storage, rotation, composition,

- 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, sandboxing, isolation, data loss prevention (DLP))7.2 Implement and operate endpoint device security
- Host-based intrusion prevention system (HIPS)
- Host-based firewalls
- Application white listing
- 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 model7.5 Operate and maintain secure virtual environments
- Hypervisor
- Virtual appliances
- Containers
- Continuity and resilience
- Attacks and countermeasures
- Shared storage

- Proofing
- Provisioning/De-provisioning
- Maintenance
- Entitlement
- Identity and access management (IAM) systems2.4 Understand and apply access controls
- Mandatory
- Discretionary
- Role-based (e.g., attribute-, subject-, object-based)
- Rule-based

3. Risk Identification, Monitoring and Analysis

- Risk visibility and reporting (e.g., risk register, sharing threat intelligence/Indicators of Compromise (IOC), Common Vulnerability Scoring (CVSS))
- Risk management concepts (e.g., impact assessments, threat modelling)
- Risk management frameworks
- Risk tolerance (e.g., appetite)
- Risk treatment (e.g., accept, transfer, mitigate, avoid)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 lifecycle3.4 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 correlation3.5 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)

generation, destruction, exchange, revocation, escrow)
- Web of Trust (WOT)

6. Network and Communications Security

- 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 protocols6.2 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 management6.5 Operate and configure network-based security devices
- Firewalls and proxies (e.g., filtering methods, web application firewalls (WAF)) Intrusion detection systems (IDS) and intrusion prevention systems (IPS)
- Network intrusion detection/prevention systems
- 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)

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.com/en-qa/

Global Knowledge, Qatar Financial Center, Burj Doha,Level 21, P.O.Box 27110, West Bay, Doha, Qatar