Systems Security Certified Practitioner
SSCP
ISC2 Certification

2024 SSCP Detailed Content Outline With Weights Final (Public Use Only)		
Last Edited August 18, 2023 - Effective Date September 15, 2024		
Classification	**Domain/Task/Subtask**	**Weight**
Domain 1	**Security Concepts and Practices**	**16%**
1.1	**Comply with codes of ethics**	
1.1.1	(ISC)2 Code of Ethics	
1.1.2	Organizational code of ethics	
1.2	**Understand security concepts**	
1.2.1	Confidentiality	
1.2.2	Integrity	
1.2.3	Availability	
1.2.4	Accountability	
1.2.5	Non-repudiation	
1.2.6	Least privilege	
1.2.7	Segregation of duties (SoD)	
1.3	**Identify and implement security controls**	
1.3.1	Technical controls (e.g., firewalls, intrusion detection systems (IDS), access control list (ACL))	
1.3.2	Physical controls (e.g., mantraps, cameras, locks)	
1.3.3	Administrative controls (e.g., security policies, standards, procedures, baselines)	
1.3.4	Assessing compliance requirements	
1.3.5	Periodic audit and review	
1.4	**Document and maintain functional security controls**	
1.4.1	Deterrent controls	
1.4.2	Preventative controls	
1.4.3	Detective controls	
1.4.4	Corrective controls	
1.4.5	Compensating controls	
1.5	**Support and implement asset management lifecycle (i.e., hardware, software, and data)**	
1.5.1	Process, planning, design, and initiation	
1.5.2	Development /Acquisition (e.g., DevSecOps, testing)	
1.5.3	Inventory and licensing (e.g., open source, closed-source)	
1.5.4	Implementation/Assessment	
1.5.5	Operation/Maintenance/End of Life (EOL)	
1.5.6	Archival and retention requirements	
1.5.7	Disposal and destruction	
1.6	**Support and/or implement change management lifecycle**	
1.6.1	Change management (e.g., roles, responsibilities, processes, communications, audit)	
1.6.2	Security impact analysis	
1.6.3	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**	**15%**
2.1	**Implement and maintain authentication methods**	
2.1.1	Single/Multi-factor authentication (MFA)	
2.1.2	Single sign-on (SSO) (e.g., Active Directory Federation Services (ADFS), OpenID Connect)	
2.1.3	Device authentication (e.g., certificate, Media Access Control (MAC) address, Trusted Platform Module (TPM))	
2.1.4	Federated access (e.g., Open Authorization 2 (OAuth2), Security Assertion Markup Language (SAML))	
2.2	**Understand and support internetwork trust architectures**	
2.2.1	Trust relationships (e.g., 1-way, 2-way, transitive, zero)	
2.2.2	Internet, intranet, extranet, and demilitarized zone (DMZ)	
2.2.3	Third-party connections (e.g., application programming interface (API), app extensions, middleware)	
2.3	**Support and/or implement the identity management lifecycle**	
2.3.1	Authorization	
2.3.2	Proofing	
2.3.3	Provisioning/De-provisioning	
2.3.4	Monitoring, Reporting, and Maintenance (e.g., role changes, new security standards)	
2.3.5	Entitlement (e.g., inherited rights, resources)	
2.3.6	Identity and access management (IAM) systems	
2.4	**Understand and administer access controls**	

2.4.1	Mandatory	
2.4.2	Discretionary	
2.4.3	Role-based (e.g., subject-based, object-based, Privileged Access Management (PAM))	
2.4.4	Rule-based	
2.4.5	Attribute-based	
Domain 3	**Risk Identification, Monitoring, and Analysis**	**15%**
3.1	**Understand risk management**	
3.1.1	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)	
3.1.2	Risk management concepts (e.g., impact assessments, threat modeling, scope)	
3.1.3	Risk management frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST))	
3.1.4	Risk tolerance (e.g., appetite, risk quantification)	
3.1.5	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**	
3.3.1	Risk management frameworks implementation	
3.3.2	Security testing	
3.3.3	Risk review (e.g., internal, supplier, architecture)	
3.3.4	Vulnerability management lifecycle (e.g., scanning, reporting, analysis, remediation)	
3.4	**Operate and monitor security platforms (e.g., continuous monitoring)**	
3.4.1	Source systems (e.g., applications, security appliances, network devices, hosts)	
3.4.2	Events of interest (e.g., errors, omissions, anomalies, unauthorized changes, compliance violations, policy failures)	
3.4.3	Log management (e.g., policy, integrity, preservation, architectures, configuration, aggregation, tuning)	
3.4.4	Security information and event management (SIEM) (e.g., real-time monitoring, analysis, tracking, audit)	
3.5	**Analyze monitoring results**	
3.5.1	Security baselines and anomalies (e.g., correlation, noise reduction)	
3.5.2	Visualizations, metrics, and trends (e.g., notifications, dashboards, timelines)	
3.5.3	Event data analysis	
3.5.4	Document and communicate findings (e.g., escalation)	
Domain 4	**Incident Response and Recovery**	**14%**
4.1	**Understand and support incident response lifecycle (e.g., National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO))**	
4.1.1	Preparation (e.g., defining roles, training programs)	
4.1.2	Detection, analysis, and escalation (e.g., incident communication, public relations)	
4.1.3	Containment	
4.1.4	Eradication	
4.1.5	Recovery (e.g., incident documentation)	
4.1.6	Post incident activities (e.g., lessons learned, new countermeasures, continuous improvement)	
4.2	**Understand and support forensic investigations**	
4.2.1	Legal (e.g., civil, criminal, administrative) and ethical principles	
4.2.2	Evidence handling (e.g., first responder, triage, chain of custody, preservation of scene)	
4.2.3	Reporting of analysis	
4.2.4	Organization Security Policy Compliance	
4.3	**Understand and support business continuity plan (BCP) and disaster recovery plan (DRP) activities**	
4.3.1	Emergency response plans and procedures (e.g., information systems contingency, pandemic, natural disaster, crisis management)	
4.3.2	Interim or alternate processing strategies	
4.3.3	Restoration planning (e.g., Restore Time Objective (RTO), Restore Point Objectives (RPO), Maximum Tolerable Downtime (MTD))	
4.3.4	Backup and redundancy implementation	
4.3.5	Testing and drills (e.g., playbook, tabletop, disaster recovery exercises, scheduling)	
Domain 5	**Cryptography**	**9%**
5.1	**Understand reasons and requirements for cryptography**	
5.1.1	Confidentiality	
5.1.2	Integrity and authenticity	
5.1.3	Data sensitivity (e.g., personally identifiable information (PII), intellectual property (IP), protected health information (PHI))	
5.1.4	Regulatory and industry best practice (e.g., Payment Card Industry Data Security Standards (PCI-DSS), International Organization for Standardization (ISO))	
5.1.5	Cryptography entropy (e.g., quantum cryptography, quantum key distribution)	
5.2	**Apply cryptography concepts**	
5.2.1	Hashing	
5.2.2	Salting	
5.2.3	Symmetric/Asymmetric encryption/Elliptic curve cryptography (ECC)	

5.2.4	Non-repudiation (e.g., digital signatures/certificates, Hash-based Message Authentication Code (HMAC), audit trails)	
5.2.5	Strength of encryption algorithms and keys (e.g., Advanced Encryption Standards (AES), Rivest-Shamir-Adleman (RSA),	
5.2.6	Cryptographic attacks and cryptanalysis	
5.3	**Understand and implement secure protocols**	
5.3.1	Services and protocols (e.g., Internet Protocol Security (IPsec), Transport Layer Security (TLS), Secure/Multipurpose Internet Mail Extensions (S/MIME), DomainKeys Identified Mail (DKIM))	
5.3.2	Common use cases (e.g., credit card processing, file transfer, web client, virtual private network (VPN), transmission of PII data)	
5.3.3	Limitations and vulnerabilities	
5.4	**Understand and support public key infrastructure (PKI) systems**	
5.4.1	Fundamental key management concepts (e.g., storage, rotation, composition, generation, destruction, exchange, revocation, escrow)	
5.4.2	Web of Trust (WOT) (e.g., Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), blockchain)	
Domain 6	**Network and Communications Security**	**16%**
6.1	**Understand and apply fundamental concepts of networking**	
6.1.1	Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models	
6.1.2	Network topologies	
6.1.3	Network relationships (e.g., peer-to-peer (P2P), client server)	
6.1.4	Transmission media types (e.g., wired, wireless)	
6.1.5	Software-defined networking (SDN) (e.g., Software-Defined Wide Area Network (SD-WAN), network virtualization, automation)	
6.1.6	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)**	
6.2.1	Countermeasures (e.g., content delivery networks (CDN), firewalls, network access controls, intrusion detection and prevention systems (IDPS))	
6.3	**Manage network access controls**	
6.3.1	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+))	
6.3.2	Remote access operation and configuration (e.g., thin client, virtual private network (VPN), virtual desktop infrastructure)	
6.4	**Manage network security**	
6.4.1	Logical and physical placement of network devices (e.g., inline, passive, virtual)	
6.4.2	Segmentation (e.g., physical/logical, data/control plane, virtual local area network (VLAN), access control list (ACL), firewall zones, micro-segmentation)	
6.4.3	Secure device management	
6.5	**Operate and configure network-based security appliances and services**	
6.5.1	Firewalls and proxies (e.g., filtering methods, web application firewall (WAF), cloud access security broker (CASB))	
6.5.2	Routers and switches	
6.5.3	Intrusion detection systems (IDS) and intrusion prevention systems (IPS)	
6.5.4	Network Access Control (NAC)	
6.5.5	Data Loss Prevention (DLP)	
6.5.6	Traffic-shaping devices (e.g., wide area network (WAN) optimization, load balancing)	
6.5.7	Unified Threat Management (UTM)	
6.6	**Secure wireless communications**	
6.6.1	Technologies (e.g., cellular network, Wi-Fi, Bluetooth, Near-Field Communication (NFC))	
6.6.2	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**	**15%**
7.1	**Identify and analyze malicious code and activity**	
7.1.1	Malware (e.g., rootkits, spyware, scareware, ransomware, trojans, virus, worms, trapdoors, backdoors, fileless, app/code/operatin3 system (OS)/mobile code vulnerabilities)	
7.1.2	Malware countermeasures (e.g., scanners, anti-malware, containment and remediation, software security)	
7.1.3	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))	
7.1.4	Malicious activity countermeasures (e.g., user awareness/training, system hardening, patching, isolation, data loss prevention (DLP))	
7.1.5	Social engineering methods (e.g., SPAM email, phishing/smishing/vishing, impersonation, scarcity, whaling)	
7.1.6	Behavior analytics (e.g., machine learning, Artificial Intelligence (AI), data analytics)	
7.2	**Implement and operate endpoint device security**	
7.2.1	Host-based intrusion prevention system (HIPS)	
7.2.2	Host-based intrusion detection system (HIDS)	
7.2.3	Host-based firewalls	
7.2.4	Application whitelisting	

7.2.5	Endpoint encryption (e.g., full disk encryption)	
7.2.6	Trusted Platform Module (TPM) (e.g., hardware security module management)	
7.2.7	Secure browsing (e.g., digital certificates)	
7.2.8	Endpoint detection and response (EDR)	
7.3	**Administer and manage mobile devices**	
7.3.1	Provisioning techniques (e.g., corporate owned, personally enabled (COPE), Bring Your Own Device (BYOD), Mobile Device Management (MDM))	
7.3.2	Containerization	
7.3.3	Encryption	
7.3.4	Mobile application management	
7.4	**Understand and configure cloud security**	
7.4.1	Deployment models (e.g., public, private, hybrid, community)	
7.4.2	Service models (e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS))	
7.4.3	Virtualization (e.g., hypervisor, Virtual Private Cloud (VPC))	
7.4.4	Legal and regulatory concerns (e.g., privacy, surveillance, data ownership, jurisdiction, eDiscovery, shadow information technology (IT))	
7.4.5	Data storage, processing, and transmission (e.g., archiving, backup, recovery, resilience)	
7.4.6	Third-party/Outsourcing requirements (e.g., service-level agreement (SLA), data portability/privacy/destruction/auditing)	
7.4.7	Shared responsibility model	
7.5	**Operate and maintain secure virtual environments**	
7.5.1	Hypervisor (i.e., Type 1 (e.g., bare metal), Type 2 (e.g., software))	
7.5.2	Virtual appliances	
7.5.3	Containers	
7.5.4	Storage management (e.g., data domain)	
7.5.5	Continuity and resilience	
7.5.6	Threats, attacks, and countermeasures (e.g., brute-force attack, virtual machine escape, threat hunting)	