Certified Security Administrator and Engineer (CSAE) Exam Objectives

Introduction

When you pass the CSAE-101 exam, you earn the CSAE certification and validate your knowledge of security administration and engineering. The CSAE-101 exam tests your knowledge of the topics tested on the CompTIA® Security+® (SY0-701) exam, along with the additional advanced objectives unique to the CSAE certification covered in this document. The CSAE certification does not require the Security+ certification as a prerequisite.

The CSAE has the knowledge and skill set required to implement security administration and engineering best practices in modern networks and systems. This professional has sufficient knowledge of network security, computer/systems security, data security, physical security, and cybersecurity allowing for the proper administration and engineering of security within these domains. The individual is aware of the security concepts, procedures, tools, and feature sets available and the capabilities they offer.

The exam is taken in the CWNP Learning Management System (LMS), and the purchase of the certification kit includes the e-learning material (covering all required knowledge), practice test, and final exam. The exam consists of 40 questions that must be answered within 100 minutes, requiring a score of 70% to earn the certification. Currently, the exam is offered only in English. While the exam has no verified prerequisites, it is recommended that the candidate have 1-3 years of experience in the networking industry and the full knowledge set tested on the CompTIA® Security+® exam.

The following table provides the breakdown of the exam as to the distribution of questions within each knowledge domain.

Knowledge Domain	**Percentage**
1 Security Concepts and Terminology	15%
2 Threats and Vulnerabilities	15%
3 Security Controls	30%
4 Security Monitoring	20%
5 Security Governance	20%

CWNP Authorized Materials Use Policy

CWNP does not condone the use of unauthorized 'training materials' such as 'brain dumps'. Individuals who utilize such materials to pass CWNP exams will have their certifications revoked. In an effort to more clearly communicate CWNP's policy on use of unauthorized study materials, CWNP directs all certification candidates to the CWNP Candidate Conduct Policy at:

http://www.cwnp.com/wp-content/uploads/pdf/CWNPCandidateConductPolicy.pdf

Please review this policy before beginning the study process for any CWNP exam.

1.0 Security Concepts and Terminology – 15%

1.1 Understand and evaluate security controls

- Security control categories and types
    - Technical controls
    - Managerial controls
    - Operational controls
    - Physical controls
- Defense-in-depth strategies
- Control effectiveness measurement and validation
- Gap analysis and remediation planning

1.2 Explain how the following core security principles apply to enterprise environments

- CIA triad implementation (Confidentiality, Integrity, Availability)
- Non-repudiation mechanisms
- AAA framework deployment (Authentication, Authorization, Accounting)
- Zero Trust architecture
- Control plane and data plane security
- Policy-driven access control systems
- Policy enforcement points

1.3 Describe and distinguish among these physical security systems

- Access control systems and badge management
- Video surveillance systems (CCTV, IP cameras)
- Environmental controls (HVAC, fire suppression)
- Physical intrusion detection sensors

- Lighting and perimeter security
- Security guard operations and integration

1.4 Describe and distinguish among these deception and disruption technologies

- Honeypot deployment and management
- Honeynet architecture design
- Honeyfile and honeytoken strategies
- Integration with threat intelligence platforms
- Deception technology for threat detection

1.5 Explain these cryptographic solutions and the roles they play in enterprise security

- PKI infrastructure deployment and management
- Certificate lifecycle management (issuance, renewal, revocation)
- Encryption implementation
    - Full-disk encryption
    - Partition encryption
    - File encryption
    - Volume encryption
    - Database encryption
    - Transport encryption
- Key management systems and HSM integration
- Digital signatures and key stretching
- Hashing and salting techniques
- Blockchain and open public ledger technologies
- Certificate management

- Certificate Authority (CA)
- Certificate Revocation List (CRL)
- Online Certificate Status Protocol (OCSP)
- Certificate Signing Request (CSR) generation

1.6 Understand how to apply change management processes for security

- Security-focused change approval workflows
- Impact analysis and risk assessment for changes
- Backout plans and rollback procedures
- Configuration management and version control
- Documentation standards for security changes
- Stakeholder management in change processes

2.0 Threats and Vulnerabilities – 15%

2.1 Analyze threat actors, attributes, and motivations

- Threat actor types
  - Nation-state actors
  - Organized crime
  - Hacktivists
  - Insider threats
  - Shadow IT
- Threat actor attribution and profiling
- Actor attributes (internal/external, resources/funding, sophistication level)
- Motivations (data exfiltration, espionage, financial gain, disruption, war)

- Attack vector analysis across multiple surfaces
- TTPs (tactics, techniques, and procedures) mapping to MITRE ATT&CK

2.2 Assess and mitigate attack vectors and surfaces

- Message-based attacks (email, SMS, instant messaging)
- Image-based and file-based attack vectors
- Voice call and removable device threats
- Social engineering campaigns (phishing, vishing, smishing, pretexting, watering hole)
- Supply chain attacks (MSPs, vendors, suppliers)
- Vulnerable and unsupported software management
- Network-based attack surfaces (wireless, wired, Bluetooth)
- Default credential and open port management

2.3 Identify and classify vulnerabilities across environments

- Application vulnerabilities (memory injection, buffer overflow, race conditions, malicious updates)
- OS-based and web-based vulnerabilities (SQL injection, XSS)
- Hardware and firmware vulnerabilities
- Virtualization vulnerabilities (VM escape, resource reuse)
- Cloud-specific and supply chain vulnerabilities
- Mobile device vulnerabilities (side loading, jailbreaking)
- Zero-day vulnerability management
- Misconfiguration identification

2.4 Analyze and respond to indicators of malicious activity

- Malware analysis

  - Ransomware
  - Trojans
  - Worms
  - Rootkits
  - Spyware
  - Bloatware
  - Viruses
  - Keyloggers
  - Logic bombs
- Physical attack indicators (brute force, RFID cloning, environmental)
- Network attack detection (DDoS, DNS attacks, wireless attacks, on-path, credential replay)
- Application attack identification (injection, buffer overflow, replay, privilege escalation, forgery, directory traversal)
- Cryptographic attack recognition (downgrade, collision, birthday)
- Password attacks (spraying, brute force)
- Behavioral indicators (account lockout, concurrent sessions, impossible travel, resource consumption, out-of-cycle logging, missing logs)

2.5 Implement comprehensive mitigation techniques

- Network segmentation and isolation strategies
- Access control lists and permission management
- Application allow listing and isolation
- Patch management programs
- Encryption and monitoring implementation

- Least privilege enforcement
- Configuration enforcement and compliance
- Secure decommissioning procedures
- Hardening techniques (encryption, endpoint protection, HIPS, port/protocol disabling, default password changes, software removal)

3.0 Security Controls – 30%

3.1 Engineer security architecture for diverse contexts

- On-premises vs. centralized vs. decentralized architecture
- Enterprise network security (network infrastructure, network edge, internetwork connectivity, physical and logical isolation/segmentation, SDN, Zero Trust architecture)
- Cloud security architecture (IaaS, PaaS, SaaS, public, private and hybrid)
- Industrial network architecture security (ICS, /SCADA, DCS, PLC, HMI, and RTOS)
- IoT system and network security
- Security for common architectural components
    - Embedded systems security
    - Infrastructure as code (IaC) security
    - Serverless and microservices security
    - Containerization security
- Architecture considerations (availability, resilience, cost, responsiveness, scalability, ease of deployment, risk transference, ease of recovery, patch management, power, compute)

3.2 Design and implement enterprise infrastructure security

- Infrastructure device considerations (placement, attributes, attack surface, connectivity, failure modes)

- Security zone design and segmentation
- Failure mode planning (fail-open vs. fail-closed)
- Network appliance deployment (jump servers, proxy servers, IPS/IDS, load balancers, sensors)
- Port security implementation (802.1X, EAP)
- Firewall architecture (WAF, UTM, NGFW, Layer 4/Layer 7)
- Selection of effective security controls

3.3 Implement secure remote communication and access solutions

- VPN architecture (site-to-site, remote access)
- Tunneling protocols (TLS, IPSec)
- SD-WAN security implementation
- SASE (Secure Access Service Edge) architecture
- Remote access security controls

3.4 Engineer comprehensive data protection strategies

- Data types and classifications
    - Regulated data
    - Trade secrets
    - Intellectual property
    - Legal information
    - Financial information
    - Sensitive data
    - Confidential data
    - Public data

    - Restricted data
    - Private data
    - Critical data
- Data state protection (at rest, in transit, in use)
- Data sovereignty and geolocation compliance
- Methods to secure data
    - Geographic restrictions
    - Encryption
    - Hashing
    - Masking
    - Tokenization
    - Obfuscation
    - Segmentation
    - Permission restrictions
    - Anonymization
- Database activity monitoring and encryption
- DLP implementation and policy tuning

3.5 Design resilience and recovery architecture

- High availability strategies (load balancing vs. clustering)
- Site resilience planning (hot, cold, warm sites)
- Geographic dispersion strategies
- Platform diversity and multi-cloud systems
- Capacity planning

- Testing (tabletop exercises, failover, simulation, parallel processing)
- Backup strategies
    - Onsite/offsite storage
    - Backup frequency
    - Backup encryption
    - Snapshots
    - Recovery procedures
    - Replication
    - Journaling
    - Media Rotation
- Power resilience (generators, UPS, redundant power supply, multiple utility feeds)

4.0 Security Monitoring – 20%

4.1 Administer secure computing resources across platforms

- Secure baseline management (establishment, deployment, maintenance)
- System hardening across multiple platforms
    - Mobile devices
    - Workstations
    - Switches and routers
    - Cloud infrastructure
    - Servers
    - ICS/SCADA
    - Embedded systems

- RTOS
- IoT devices

- Wireless device security (site surveys, heat maps, WPA3, AAA/RADIUS, authentication protocols)
- Mobile device management (MDM deployment, BYOD/COPE/CYOD, mobile policies, application distribution)
- Application security (input validation, secure cookies, code analysis, code signing, sandboxing)

4.2 Manage assets throughout the lifecycle

- Acquisition and procurement (security requirements, vendor evaluation, supply chain security)
- Assignment and classification
- Monitoring and tracking (inventory, enumeration, change tracking, license management)
- Disposal and decommissioning (sanitization, destruction, certification, retention compliance)

4.3 Implement and operate vulnerability management programs

- Vulnerability identification methods
  - Vulnerability scanning (authenticated, unauthenticated)
  - Application security testing (SAST, DAST, SCA)
  - Threat feed integration
  - Penetration testing
  - Bug bounty programs
  - System and process audits

- Vulnerability analysis (confirmation, CVSS/CVE, OSV, classification, prioritization, environmental factors, risk alignment)
- Remediation and validation (patching programs, compensating controls, exceptions, verification testing)
- Vulnerability reporting

4.4 Deploy and manage security monitoring systems

- SIEM (deployment, configuration, management, tuning)
- XDR (extended detection and response)
- Log management (aggregation, correlation, analysis, retention)
- Alert management (generation, tuning, response workflows)
- Compliance monitoring (SCAP security content automation scanning, benchmarks, drift detection)
- Monitoring tools deployment
    - Antivirus and anti-malware
    - Data Loss Prevention (DLP)
    - SNMP traps
    - NetFlow
    - Network taps
    - Packet capture systems
- Reporting and dashboards

4.5 Engineer and operate advanced security capabilities

- Network security capabilities
    - Firewall management (rules, ACLs, ports/protocols, screened subnets)
    - IPS/IDS administration (trends, signatures, active vs. passive)

    - Network Access Control (NAC)
- Content filtering and inspection
    - Web filtering (agent-based, proxy, URL scanning, reputation)
    - DNS filtering (sinkholing, threat protection)
    - Email security (DMARC, DKIM, SPF, gateway)
- Operating system security (Group Policy, SELinux, security baselines)
- Protocol security (secure protocols, TLS versions, cipher suites)
- Endpoint security (EDR/XDR, UEBA)
- File integrity monitoring

4.6 Administer identity and access management systems

- User lifecycle management (provisioning, de-provisioning, least privilege)
- Identity proofing and verification
- Federation and SSO (LDAP, OAuth, SAML, OpenID Connect)
- Access control models (MAC, DAC, RBAC, ABAC)
- Multi-factor authentication (implementations, factors, risk-based authentication)
- Password management (policy enforcement, passwordless authentication)
- Privileged Access Management
    - PAM platform deployment
    - Just-in-time (JIT) access
    - Password vaulting
    - Session management
    - Account discovery
- Access reviews and attestation

4.7 Implement security automation and orchestration

- Automation use cases (provisioning, guardrails, ticketing, vulnerability scanning, compliance checking)
- Integration capabilities (APIs, webhooks, custom scripts)
- CI/CD security automation (scanning, testing, compliance gates)
- Benefits and considerations

4.8 Execute incident response operations

- Incident response process (preparation, detection, containment, eradication, recovery, lessons learned)
- Training and testing (tabletop exercises, simulations, debriefs)
- Root cause analysis
- Threat hunting (hypothesis-driven, intelligence-driven, baseline deviation)
- Digital forensics (chain of custody, acquisition, preservation, analysis, reporting)

4.9 Conduct security investigations

- Log analysis
    - Firewall logs
    - Application logs
    - Endpoint logs
    - OS-specific security logs
    - IPS/IDS logs
    - Network logs
    - Metadata
- Data source correlation (SIEM, vulnerability scans, packet captures, threat intelligence)
- Investigation documentation

5.0 Security Governance – 20%

5.1 Implement effective security governance frameworks

- Policies and standards development
    - Acceptable Use Policy (AUP)
    - Information security policies
    - Business continuity policy
    - Disaster recovery policy
    - SDLC policy
    - Access control standards
    - Encryption standards
- Procedures (change management, onboarding/offboarding, playbooks)
- External considerations (regulatory, legal, industry standards, geographic scope)
- Governance structures (board oversight, committees, governance models)
- Roles and responsibilities (owners, controllers, processors, custodians, responsibility matrices)
- Monitoring and revision

5.2 Manage organizational risk through structured processes

- Risk identification
- Risk assessment (ad hoc, recurring, continuous)
- Risk analysis
    - Qualitative analysis (probability, impact, risk matrix)
    - Quantitative analysis (SLE, ALE, ARO)

    - Environmental variables
- Risk register management
- Risk tolerance and appetite
- Risk treatment strategies
    - Risk transfer
    - Risk acceptance (exemptions, exceptions)
    - Risk avoidance
    - Risk mitigation
- Risk reporting
- Business impact analysis (RTO, RPO, MTTR, MTBF)

5.3 Administer third-party risk management programs

- Vendor assessment (questionnaires, audits, certifications)
- Supply chain analysis (mapping, dependencies, fourth-party risk)
- Vendor selection and due diligence
- Agreement management
    - Service Level Agreement (SLA)
    - Memorandum of Agreement (MOA)
    - Memorandum of Understanding (MOU)
    - Master Service Agreement (MSA)
    - Statement of Work (SOW)
    - Non-Disclosure Agreement (NDA)
    - Business Partnership Agreement (BPA)
    - Data Processing Agreement (DPA)

- Ongoing monitoring
- Rules of engagement

5.4 Maintain comprehensive compliance programs

- Compliance reporting and monitoring
- Automation and dashboards
- Privacy compliance programs
    - GDPR (General Data Protection Regulation)
    - CCPA (California Consumer Privacy Act)
    - HIPAA (Health Insurance Portability and Accountability Act)
    - PCI DSS (Payment Card Industry Data Security Standard)
- Data governance (inventory, classification, retention)
- Attestation processes
- Internal audits (compliance assessments, control testing, gap analysis)
- External audit coordination (regulatory exams, financial audits, third-party assessments)

5.5 Conduct security assessments and testing

- Internal assessments (compliance, controls, vulnerabilities, architecture)
- Audit coordination
- Penetration testing programs
    - Testing types (physical, network, application, social engineering)
    - Testing methodologies (offensive, defensive, integrated)
    - Testing environments (known, partially-known, unknown)
    - Testing phases (planning, reconnaissance, exploitation, reporting)
- Reconnaissance operations

- Passive reconnaissance (OSINT, DNS enumeration, social media)
- Active reconnaissance (port scanning, service enumeration, network mapping)

5.6 Implement security awareness and culture programs

- Training programs
  - Delivery methods (CBT, instructor-led, microlearning, newsletters)
  - Content topics (phishing, social engineering, password security, data handling, OPSEC)
- Phishing simulations (campaign design, execution, metrics, remedial training)
- Policy communication
- User guidance (quick reference guides, job aids, role-specific guides)
- Situational awareness (threat notifications, advisories)
- Reporting procedures (incident reporting, anonymous channels)
- Culture development
  - Security champions programs
  - Gamification and incentives
  - Awareness metrics
  - Executive sponsorship
