CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives

EXAM NUMBER: CAS-004

CompTIA

About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA Advanced Security Practitioner (CASP+) (CAS-004) certification exam. The CompTIA CASP+ certification exam will verify the successful candidate has the knowledge and skills required to:

- **Architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise**
- **Use monitoring, detection, incident response, and automation to proactively support ongoing security operations in an enterprise environment**
- **Apply security practices to cloud, on-premises, endpoint, and mobile infrastructure, while considering cryptographic technologies and techniques**
- **Consider the impact of governance, risk, and compliance requirements throughout the enterprise**

This is equivalent to at least ten years of general hands-on IT experience, with at least five of those years being broad hands-on security experience. These content examples are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

EXAM ACCREDITATION

The CompTIA CASP+ (CAS-004) exam is accredited by ANSI to show compliance with the ISO 17024 standard and, as such, undergoes regular reviews and updates to the exam objectives.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an entry-level IT professional.

CompTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka "brain dumps"). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the **CompTIA Certification Exam Policies**. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the **CompTIA Candidate Agreement**. If a candidate has a question as to whether study materials are considered unauthorized (aka "brain dumps"), he/she should contact CompTIA at **examsecurity@comptia.org** to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	CAS-004
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	165 minutes
Recommended experience	• Minimum of ten years of general hands-on IT experience, with at least five of those years being broad hands-on IT security experience • Network+, Security+, CySA+, Cloud+, and PenTest+ or equivalent certifications/knowledge
Passing score	Pass/Fail only — no scaled score

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Security Architecture	29%
2.0 Security Operations	30%
3.0 Security Engineering and Cryptography	26%
4.0 Governance, Risk, and Compliance	15%
Total	**100%**

1.0 Security Architecture

1.1 Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.

- **Services**
  - Load balancer
  - Intrusion detection system (IDS)/network intrusion detection system (NIDS)/wireless intrusion detection system (WIDS)
  - Intrusion prevention system (IPS)/network intrusion prevention system (NIPS)/wireless intrusion prevention system (WIPS)
  - Web application firewall (WAF)
  - Network access control (NAC)
  - Virtual private network (VPN)
  - Domain Name System Security Extensions (DNSSEC)
  - Firewall/unified threat management (UTM)/next-generation firewall (NGFW)
  - Network address translation (NAT) gateway
  - Internet gateway
  - Forward/transparent proxy
  - Reverse proxy
  - Distributed denial-of-service (DDoS) protection
  - Routers
  - Mail security
  - Application programming interface (API) gateway/Extensible Markup Language (XML) gateway
  - Traffic mirroring
    - Switched port analyzer (SPAN) ports
    - Port mirroring
    - Virtual private cloud (VPC)
    - Network tap
  - Sensors
    - Security information and event management (SIEM)
    - File integrity monitoring (FIM)
    - Simple Network Management Protocol (SNMP) traps
    - NetFlow
    - Data loss prevention (DLP)
    - Antivirus
- **Segmentation**
  - Microsegmentation
  - Local area network (LAN)/virtual local area network (VLAN)
  - Jump box
  - Screened subnet
  - Data zones
  - Staging environments
  - Guest environments
  - VPC/virtual network (VNET)
  - Availability zone
  - NAC lists
  - Policies/security groups
  - Regions
  - Access control lists (ACLs)
  - Peer-to-peer
  - Air gap
- **Deperimeterization/zero trust**
  - Cloud
  - Remote work
  - Mobile
  - Outsourcing and contracting
  - Wireless/radio frequency (RF) networks
- **Merging of networks from various organizations**
  - Peering
  - Cloud to on premises
  - Data sensitivity levels
  - Mergers and acquisitions
  - Cross-domain
  - Federation
  - Directory services
- **Software-defined networking (SDN)**
  - Open SDN
  - Hybrid SDN
  - SDN overlay

1.2 Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.

- **Scalability**
  - Vertically
  - Horizontally
- **Resiliency**
  - High availability
  - Diversity/heterogeneity
  - Course of action orchestration
  - Distributed allocation
  - Redundancy
  - Replication
  - Clustering
- **Automation**
  - Autoscaling
  - Security Orchestration, Automation, and Response (SOAR)
  - Bootstrapping
- **Performance**
- **Containerization**
- **Virtualization**
- **Content delivery network**
- **Caching**

1.3 Given a scenario, integrate software applications securely into an enterprise architecture.

- **Baseline and templates**
  - Secure design patterns/ types of web technologies
    - Storage design patterns
  - Container APIs
  - Secure coding standards
  - Application vetting processes
  - API management
  - Middleware
- **Software assurance**
  - Sandboxing/development environment
  - Validating third-party libraries
  - Defined DevOps pipeline
  - Code signing
  - Interactive application security testing (IAST) vs. dynamic application security testing (DAST) vs. static application security testing (SAST)
- **Considerations of integrating enterprise applications**
  - Customer relationship management (CRM)
  - Enterprise resource planning (ERP)
  - Configuration management database (CMDB)
  - Content management system (CMS)
  - Integration enablers
    - Directory services
    - Domain name system (DNS)
    - Service-oriented architecture (SOA)
    - Enterprise service bus (ESB)
- **Integrating security into development life cycle**
  - Formal methods
  - Requirements
  - Fielding
  - Insertions and upgrades
  - Disposal and reuse
  - Testing
    - Regression
    - Unit testing
    - Integration testing
  - Development approaches
    - SecDevOps
    - Agile
    - Waterfall
    - Spiral
    - Versioning
    - Continuous integration/ continuous delivery (CI/CD) pipelines
  - Best practices
    - Open Web Application Security Project (OWASP)
    - Proper Hypertext Transfer Protocol (HTTP) headers

1.4 Given a scenario, implement data security techniques for securing enterprise architecture.

- **Data loss prevention**
  - Blocking use of external media
  - Print blocking
  - Remote Desktop Protocol (RDP) blocking
  - Clipboard privacy controls
  - Restricted virtual desktop infrastructure (VDI) implementation
  - Data classification blocking
- **Data loss detection**
  - Watermarking
  - Digital rights management (DRM)
  - Network traffic decryption/ deep packet inspection
  - Network traffic analysis
- **Data classification, labeling, and tagging**
  - Metadata/attributes
- **Obfuscation**
  - Tokenization
  - Scrubbing
  - Masking
- **Anonymization**
- **Encrypted vs. unencrypted**
- **Data life cycle**
  - Create
  - Use
  - Share
  - Store
  - Archive
  - Destroy
- **Data inventory and mapping**
- **Data integrity management**
- **Data storage, backup, and recovery**
  - Redundant array of inexpensive disks (RAID)

1.5 Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.

- **Credential management**
  - Password repository application
    - End-user password storage
    - On premises vs. cloud repository
  - Hardware key manager
  - Privileged access management
- **Password policies**
  - Complexity
  - Length
  - Character classes
  - History
  - Maximum/minimum age
  - Auditing
  - Reversable encryption
- **Federation**
  - Transitive trust
  - OpenID
  - Security Assertion Markup Language (SAML)
  - Shibboleth
- **Access control**
  - Mandatory access control (MAC)
  - Discretionary access control (DAC)
  - Role-based access control
  - Rule-based access control
  - Attribute-based access control
- **Protocols**
  - Remote Authentication Dial-in User Server (RADIUS)
  - Terminal Access Controller Access Control System (TACACS)
  - Diameter
  - Lightweight Directory Access Protocol (LDAP)
  - Kerberos
  - OAuth
  - 802.1X
  - Extensible Authentication Protocol (EAP)
- **Multifactor authentication (MFA)**
  - Two-factor authentication (2FA)
  - 2-Step Verification
  - In-band
  - Out-of-band
- **One-time password (OTP)**
  - HMAC-based one-time password (HOTP)
  - Time-based one-time password (TOTP)
- **Hardware root of trust**
- **Single sign-on (SSO)**
- **JavaScript Object Notation (JSON) web token (JWT)**
- **Attestation and identity proofing**

1.6 Given a set of requirements, implement secure cloud and virtualization solutions.

- **Virtualization strategies**
  - Type 1 vs. Type 2 hypervisors
  - Containers
  - Emulation
  - Application virtualization
  - VDI
- **Provisioning and deprovisioning**
- **Middleware**
- **Metadata and tags**
- **Deployment models and considerations**
  - Business directives
    - Cost
    - Scalability
    - Resources
    - Location
    - Data protection
  - Cloud deployment models
    - Private
    - Public
    - Hybrid
    - Community
- **Hosting models**
  - Multitenant
  - Single-tenant
- **Service models**
  - Software as a service (SaaS)
  - Platform as a service (PaaS)
  - Infrastructure as a service (IaaS)
- **Cloud provider limitations**
  - Internet Protocol (IP) address scheme
  - VPC peering
- **Extending appropriate on-premises controls**
- **Storage models**
  - Object storage/file-based storage
  - Database storage
  - Block storage
  - Blob storage
  - Key-value pairs

1.7 Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.

- **Privacy and confidentiality requirements**
- **Integrity requirements**
- **Non-repudiation**
- **Compliance and policy requirements**
- **Common cryptography use cases**
  - Data at rest
  - Data in transit
  - Data in process/data in use
  - Protection of web services
  - Embedded systems
  - Key escrow/management
  - Mobile security
  - Secure authentication
  - Smart card
- **Common PKI use cases**
  - Web services
  - Email
  - Code signing
  - Federation
  - Trust models
  - VPN
  - Enterprise and security automation/orchestration

1.8 Explain the impact of emerging technologies on enterprise security and privacy.

- **Artificial intelligence**
- **Machine learning**
- **Quantum computing**
- **Blockchain**
- **Homomorphic encryption**
  - Private information retrieval
  - Secure function evaluation
  - Private function evaluation
- **Secure multiparty computation**
- **Distributed consensus**
- **Big Data**
- **Virtual/augmented reality**
- **3-D printing**
- **Passwordless authentication**
- **Nano technology**
- **Deep learning**
  - Natural language processing
  - Deep fakes
- **Biometric impersonation**

2.0 Security Operations

2.1 Given a scenario, perform threat management activities.

- **Intelligence types**
  - Tactical
    - Commodity malware
  - Strategic
    - Targeted attacks
  - Operational
    - Threat hunting
    - Threat emulation
- **Actor types**
  - Advanced persistent threat (APT)/nation-state
  - Insider threat
  - Competitor
  - Hacktivist
  - Script kiddie
  - Organized crime
- **Threat actor properties**
  - Resource
    - Time
    - Money
  - Supply chain access
  - Create vulnerabilities
  - Capabilities/sophistication
  - Identifying techniques
- Intelligence collection methods
  - Intelligence feeds
  - Deep web
  - Proprietary
  - Open-source intelligence (OSINT)
  - Human intelligence (HUMINT)
- **Frameworks**
  - MITRE Adversarial Tactics, Techniques, & Common knowledge (ATT&CK)
    - ATT&CK for industrial control system (ICS)
  - Diamond Model of Intrusion Analysis
  - Cyber Kill Chain

2.2 Given a scenario, analyze indicators of compromise and formulate an appropriate response.

- **Indicators of compromise**
  - Packet capture (PCAP)
  - Logs
    - Network logs
    - Vulnerability logs
    - Operating system logs
    - Access logs
    - NetFlow logs
  - Notifications
    - FIM alerts
    - SIEM alerts
    - DLP alerts
    - IDS/IPS alerts
    - Antivirus alerts
  - Notification severity/priorities
  - Unusual process activity
- **Response**
  - Firewall rules
  - IPS/IDS rules
  - ACL rules
  - Signature rules
  - Behavior rules
  - DLP rules
  - Scripts/regular expressions

2.3 Given a scenario, perform vulnerability management activities.

- **Vulnerability scans**
  - Credentialed vs. non-credentialed
  - Agent-based/server-based
  - Criticality ranking
  - Active vs. passive
- **Security Content Automation Protocol (SCAP)**
  - Extensible Configuration Checklist Description Format (XCCDF)
  - Open Vulnerability and Assessment Language (OVAL)
  - Common Platform Enumeration (CPE)
  - Common Vulnerabilities and Exposures (CVE)
  - Common Vulnerability Scoring System (CVSS)
  - Common Configuration Enumeration (CCE)
  - Asset Reporting Format (ARF)
- **Self-assessment vs. third-party vendor assessment**
- **Patch management**
- **Information sources**
  - Advisories
  - Bulletins
  - Vendor websites
  - Information Sharing and Analysis Centers (ISACs)
  - News reports

2.4 Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools.

- **Methods**
  - Static analysis
  - Dynamic analysis
  - Side-channel analysis
  - Reverse engineering
    - Software
    - Hardware
  - Wireless vulnerability scan
  - Software composition analysis
  - Fuzz testing
  - Pivoting
  - Post-exploitation
  - Persistence
- **Tools**
  - SCAP scanner
  - Network traffic analyzer
  - Vulnerability scanner
  - Protocol analyzer
  - Port scanner
  - HTTP interceptor
  - Exploit framework
  - Password cracker
- **Dependency management**
- **Requirements**
  - Scope of work
  - Rules of engagement
  - Invasive vs. non-invasive
  - Asset inventory
  - Permissions and access
  - Corporate policy considerations
  - Facility considerations
  - Physical security considerations
  - Rescan for corrections/changes

2.5 Given a scenario, analyze vulnerabilities and recommend risk mitigations.

- **Vulnerabilities**
  - Race conditions
  - Overflows
    - Buffer
    - Integer
  - Broken authentication
  - Unsecure references
  - Poor exception handling
  - Security misconfiguration
  - Improper headers
  - Information disclosure
  - Certificate errors
  - Weak cryptography implementations
  - Weak ciphers
  - Weak cipher suite implementations
  - Software composition analysis
  - Use of vulnerable frameworks and software modules
  - Use of unsafe functions
  - Third-party libraries
    - Dependencies
  - Code injections/malicious changes
  - End of support/end of life
  - Regression issues
- **Inherently vulnerable system/application**
  - Client-side processing vs. server-side processing
  - JSON/representational state transfer (REST)
  - Browser extensions
    - Flash
    - ActiveX
  - Hypertext Markup Language 5 (HTML5)
  - Asynchronous JavaScript and XML (AJAX)
  - Simple Object Access Protocol (SOAP)
  - Machine code vs. bytecode or interpreted vs. emulated
- **Attacks**
  - Directory traversal
  - Cross-site scripting (XSS)
  - Cross-site request forgery (CSRF)
  - Injection
    - XML
    - LDAP
    - Structured Query Language (SQL)
    - Command
    - Process
  - Sandbox escape
  - Virtual machine (VM) hopping
  - VM escape
  - Border Gateway Protocol (BGP)/ route hijacking
  - Interception attacks
  - Denial-of-service (DoS)/DDoS
  - Authentication bypass
  - Social engineering
  - VLAN hopping

2.6 Given a scenario, use processes to reduce risk.

- **Proactive and detection**
  - Hunts
  - Developing countermeasures
  - Deceptive technologies
    - Honeynet
    - Honeypot
    - Decoy files
    - Simulators
    - Dynamic network configurations
- **Security data analytics**
  - Processing pipelines
    - Data
    - Stream
  - Indexing and search
  - Log collection and curation
  - Database activity monitoring
- **Preventive**
  - Antivirus
  - Immutable systems
  - Hardening
  - Sandbox detonation
- **Application control**
  - License technologies
  - Allow list vs. block list
  - Time of check vs. time of use
  - Atomic execution
- **Security automation**
  - Cron/scheduled tasks
  - Bash
  - PowerShell
  - Python
- **Physical security**
  - Review of lighting
  - Review of visitor logs
  - Camera reviews
  - Open spaces vs. confined spaces

2.7 Given an incident, implement the appropriate response.

- **Event classifications**
  - False positive
  - False negative
  - True positive
  - True negative
- **Triage event**
- **Preescalation tasks**
- **Incident response process**
  - Preparation
  - Detection
  - Analysis
  - Containment
  - Recovery
  - Lessons learned
- **Specific response playbooks/processes**
  - Scenarios
    - Ransomware
    - Data exfiltration
    - Social engineering
  - Non-automated response methods
  - Automated response methods
    - Runbooks
    - SOAR
- **Communication plan**
- **Stakeholder management**

2.8 Explain the importance of forensic concepts.

- **Legal vs. internal corporate purposes**
- **Forensic process**
  - Identification
  - Evidence collection
    - Chain of custody
    - Order of volatility
      - Memory snapshots
      - Images
    - Cloning
  - Evidence preservation
    - Secure storage
    - Backups
  - Analysis
    - Forensics tools
  - Verification
  - Presentation
- **Integrity preservation**
  - Hashing
- **Cryptanalysis**
- **Steganalysis**

2.9 Given a scenario, use forensic analysis tools.

- **File carving tools**
  - Foremost
  - Strings
- **Binary analysis tools**
  - Hex dump
  - Binwalk
  - Ghidra
  - GNU Project debugger (GDB)
  - OllyDbg
  - readelf
  - objdump
  - strace
  - ldd
  - file
- **Analysis tools**
  - ExifTool
  - Nmap
  - Aircrack-ng
  - Volatility
  - The Sleuth Kit
  - Dynamically vs. statically linked
- **Imaging tools**
  - Forensic Toolkit (FTK) Imager
  - dd
- **Hashing utilities**
  - sha256sum
  - ssdeep
- **Live collection vs. post-mortem tools**
  - netstat
  - ps
  - vmstat
  - ldd
  - lsof
  - netcat
  - tcpdump
  - conntrack
  - Wireshark

3.0 Security Engineering and Cryptography

3.1 Given a scenario, apply secure configurations to enterprise mobility.

- **Managed configurations**
  - Application control
  - Password
  - MFA requirements
  - Token-based access
  - Patch repository
  - Firmware Over-the-Air
  - Remote wipe
  - WiFi
    - WiFi Protected Access (WPA2/3)
    - Device certificates
  - Profiles
  - Bluetooth
  - Near-field communication (NFC)
  - Peripherals
  - Geofencing
  - VPN settings
  - Geotagging
  - Certificate management
  - Full device encryption
  - Tethering
  - Airplane mode
  - Location services
  - DNS over HTTPS (DoH)
  - Custom DNS
- **Deployment scenarios**
  - Bring your own device (BYOD)
  - Corporate-owned
  - Corporate owned, personally enabled (COPE)
  - Choose your own device (CYOD)
- **Security considerations**
  - Unauthorized remote activation/ deactivation of devices or features
  - Encrypted and unencrypted communication concerns
  - Physical reconnaissance
  - Personal data theft
  - Health privacy
  - Implications of wearable devices
  - Digital forensics of collected data
  - Unauthorized application stores
  - Jailbreaking/rooting
  - Side loading
  - Containerization
  - Original equipment manufacturer (OEM) and carrier differences
  - Supply chain issues
  - eFuse

3.2 Given a scenario, configure and implement endpoint security controls.

- **Hardening techniques**
  - Removing unneeded services
  - Disabling unused accounts
  - Images/templates
  - Remove end-of-life devices
  - Remove end-of-support devices
  - Local drive encryption
  - Enable no execute (NX)/ execute never (XN) bit
  - Disabling central processing unit (CPU) virtualization support
  - Secure encrypted enclaves/ memory encryption
  - Shell restrictions
  - Address space layout randomization (ASLR)
- **Processes**
  - Patching
    - Firmware
    - Application
  - Logging
  - Monitoring
- **Mandatory access control**
  - Security-Enhanced Linux (SELinux)/ Security-Enhanced Android (SEAndroid)
  - Kernel vs. middleware
- **Trustworthy computing**
  - Trusted Platform Module (TPM)
  - Secure Boot
  - Unified Extensible Firmware Interface (UEFI)/basic input/ output system (BIOS) protection
  - Attestation services
  - Hardware security module (HSM)
  - Measured boot
  - Self-encrypting drives (SEDs)
- **Compensating controls**
  - Antivirus
  - Application controls
  - Host-based intrusion detection system (HIDS)/Host-based intrusion prevention system (HIPS)
  - Host-based firewall
  - Endpoint detection and response (EDR)
  - Redundant hardware
  - Self-healing hardware
  - User and entity behavior analytics (UEBA)

3.3 Explain security considerations impacting specific sectors and operational technologies.

- **Embedded**
  - Internet of Things (IoT)
  - System on a chip (SoC)
  - Application-specific integrated circuit (ASIC)
  - Field-programmable gate array (FPGA)
- **ICS/supervisory control and data acquisition (SCADA)**
  - Programmable logic controller (PLC)
  - Historian
  - Ladder logic
  - Safety instrumented system
  - Heating, ventilation, and air conditioning (HVAC)
- **Protocols**
  - Controller Area Network (CAN) bus
  - Modbus
  - Distributed Network Protocol 3 (DNP3)
  - Zigbee
  - Common Industrial Protocol (CIP)
  - Data distribution service
- **Sectors**
  - Energy
  - Manufacturing
  - Healthcare
  - Public utilities
  - Public services
  - Facility services

3.4 Explain how cloud technology adoption impacts organizational security.

- **Automation and orchestration**
- **Encryption configuration**
- **Logs**
  - Availability
  - Collection
  - Monitoring
  - Configuration
  - Alerting
- **Monitoring configurations**
- **Key ownership and location**
- **Key life-cycle management**
- **Backup and recovery methods**
  - Cloud as business continuity and disaster recovery (BCDR)
  - Primary provider BCDR
  - Alternative provider BCDR
- **Infrastructure vs. serverless computing**
- **Application virtualization**
- **Software-defined networking**
- **Misconfigurations**
- **Collaboration tools**
- **Storage configurations**
  - Bit splitting
  - Data dispersion
- **Cloud access security broker (CASB)**

3.5 Given a business requirement, implement the appropriate PKI solution.

- **PKI hierarchy**
  - Certificate authority (CA)
  - Subordinate/intermediate CA
  - Registration authority (RA)
- **Certificate types**
  - Wildcard certificate
  - Extended validation
  - Multidomain
  - General purpose
- **Certificate usages/profiles/templates**
  - Client authentication
  - Server authentication
  - Digital signatures
  - Code signing
- **Extensions**
  - Common name (CN)
  - Storage area network (SAN)
- **Trusted providers**
- **Trust model**
- **Cross-certification**
- **Configure profiles**
- **Life-cycle management**
- **Public and private keys**
- **Digital signature**
- **Certificate pinning**
- **Certificate stapling**
- **Corporate signing requests (CSRs)**
- **Online Certificate Status Protocol (OCSP) vs. certificate revocation list (CRL)**
- **HTTP Strict Transport Security (HSTS)**

3.6 Given a business requirement, implement the appropriate cryptographic protocols and algorithms.

- **Hashing**
  - Secure Hashing Algorithm (SHA)
  - Hash-based message authentication code (HMAC)
  - Message digest (MD)
  - RACE integrity primitives evaluation message digest (RIPEMD)
  - Poly1305
- **Symmetric algorithms**
  - Modes of operation
    - Galois/Counter Mode (GCM)
    - Electronic codebook (ECB)
    - Cipher block chaining (CBC)
    - Counter (CTR)
    - Output feedback (OFB)
  - Stream and block
    - Advanced Encryption Standard (AES)
    - Triple digital encryption standard (3DES)
    - ChaCha
    - Salsa20
- **Asymmetric algorithms**
  - Key agreement
    - Diffie-Hellman
    - Elliptic-curve Diffie-Hellman (ECDH)
  - Signing
    - Digital signature algorithm (DSA)
    - Rivest, Shamir, and Adleman (RSA)
    - Elliptic-curve digital signature algorithm (ECDSA)
- **Protocols**
  - Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)
  - Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Internet Protocol Security (IPSec)
  - Secure Shell (SSH)
  - EAP
- **Elliptic curve cryptography**
  - P256
  - P384
- **Forward secrecy**
- **Authenticated encryption with associated data**
- **Key stretching**
  - Password-based key derivation function 2 (PBKDF2)
  - Bcrypt

3.7 Given a scenario, troubleshoot issues with cryptographic implementations.

- **Implementation and configuration issues**
  - Validity dates
  - Wrong certificate type
  - Revoked certificates
  - Incorrect name
  - Chain issues
    - Invalid root or intermediate CAs
    - Self-signed
  - Weak signing algorithm
  - Weak cipher suite
  - Incorrect permissions
  - Cipher mismatches
  - Downgrade
- **Keys**
  - Mismatched
  - Improper key handling
  - Embedded keys
  - Rekeying
  - Exposed private keys
  - Crypto shredding
  - Cryptographic obfuscation
  - Key rotation
  - Compromised keys

4.0 Governance, Risk, and Compliance

4.1 Given a set of requirements, apply the appropriate risk strategies.

- **Risk assessment**
  - Likelihood
  - Impact
  - Qualitative vs. quantitative
  - Exposure factor
  - Asset value
  - Total cost of ownership (TCO)
  - Return on investment (ROI)
  - Mean time to recovery (MTTR)
  - Mean time between failure (MTBF)
  - Annualized loss expectancy (ALE)
  - Annualized rate of occurrence (ARO)
  - Single loss expectancy (SLE)
  - Gap analysis
- **Risk handling techniques**
  - Transfer
  - Accept
  - Avoid
  - Mitigate
- **Risk types**
  - Inherent
  - Residual
  - Exceptions
- **Risk management life cycle**
  - Identify
  - Assess
  - Control
    - People
    - Process
    - Technology
    - Protect
    - Detect
    - Respond
    - Restore
  - Review
  - Frameworks
- **Risk tracking**
  - Risk register
  - Key performance indicators
    - Scalability
    - Reliability
    - Availability
  - Key risk indicators
- **Risk appetite vs. risk tolerance**
  - Tradeoff analysis
  - Usability vs. security requirements
- **Policies and security practices**
  - Separation of duties
  - Job rotation
  - Mandatory vacation
  - Least privilege
  - Employment and termination procedures
  - Training and awareness for users
  - Auditing requirements and frequency

4.2 Explain the importance of managing and mitigating vendor risk.

- **Shared responsibility model (roles/responsibilities)**
  - Cloud service provider (CSP)
    - Geographic location
    - Infrastructure
    - Compute
    - Storage
    - Networking
    - Services
  - Client
    - Encryption
    - Operating systems
    - Applications
    - Data
- **Vendor lock-in and vendor lockout**
- **Vendor viability**
  - Financial risk
  - Merger or acquisition risk
- **Meeting client requirements**
  - Legal
  - Change management
  - Staff turnover
  - Device and technical configurations
- **Support availability**
- **Geographical considerations**
- **Supply chain visibility**
- **Incident reporting requirements**
- **Source code escrows**
- **Ongoing vendor assessment tools**
- **Third-party dependencies**
  - Code
  - Hardware
  - Modules
- **Technical considerations**
  - Technical testing
  - Network segmentation
  - Transmission control
  - Shared credentials

4.3 Explain compliance frameworks and legal considerations, and their organizational impact.

- **Security concerns of integrating diverse industries**
- **Data considerations**
  - Data sovereignty
  - Data ownership
  - Data classifications
  - Data retention
  - Data types
    - Health
    - Financial
    - Intellectual property
    - Personally identifiable information (PII)
  - Data removal, destruction, and sanitization
- **Geographic considerations**
  - Location of data
  - Location of data subject
  - Location of cloud provider
- **Third-party attestation of compliance**
- **Regulations, accreditations, and standards**
  - Payment Card Industry Data Security Standard (PCI DSS)
  - General Data Protection Regulation (GDPR)
  - International Organization for Standardization (ISO)
  - Capability Maturity Model Integration (CMMI)
  - National Institute of Standards and Technology (NIST)
  - Children's Online Privacy Protection Act (COPPA)
  - Common Criteria
  - Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR)
- **Legal considerations**
  - Due diligence
  - Due care
  - Export controls
  - Legal holds
  - E-discovery
- **Contract and agreement types**
  - Service-level agreement (SLA)
  - Master service agreement (MSA)
  - Non-disclosure agreement (NDA)
  - Memorandum of understanding (MOU)
  - Interconnection security agreement (ISA)
  - Operational-level agreement
  - Privacy-level agreement

4.4 Explain the importance of business continuity and disaster recovery concepts.

- **Business impact analysis**
  - Recovery point objective
  - Recovery time objective
  - Recovery service level
  - Mission essential functions
- **Privacy impact assessment**
- **Disaster recovery plan (DRP)/ business continuity plan (BCP)**
  - Cold site
  - Warm site
  - Hot site
  - Mobile site
- **Incident response plan**
  - Roles/responsibilities
  - After-action reports
- **Testing plans**
  - Checklist
  - Walk-through
  - Tabletop exercises
  - Full interruption test
  - Parallel test/simulation test

CASP+ (CAS-004) Acronym List

The following is a list of acronyms that appear on the CompTIA CASP+ certification exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	SPELLED OUT
2FA	Two-Factor Authentication
3DES	Triple Digital Encryption Standard
ACL	Access Control List
AES	Advanced Encryption Standard
AJAX	Asynchronous JavaScript and XML
ALE	Annualized Loss Expectancy
API	Application Programming Interface
APT	Advanced Persistent Threat
ARF	Asset Reporting Format
ARO	Annualized Rate of Occurrence
ASIC	Application-Specific Integrated Circuit
ASLR	Address Space Layout Randomization
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
BCDR	Business Continuity and Disaster Recovery
BCP	Business Continuity Plan
BGP	Border Gateway Protocol
BIOS	Basic Input/Output System
BYOD	Bring Your Own Device
CA	Certificate Authority
CAN	Controller Area Network
CASB	Cloud Access Security Broker
CBC	Cipher Block Chaining
CCE	Common Configuration Enumeration
CI/CD	Continuous Integration/Continuous Delivery
CIP	Common Industrial Protocol
CMDB	Configuration Database Management
CMMI	Capability Maturity Model Integration
CN	Common Name
COPE	Corporate Owned, Personally Enabled
COPPA	Children's Online Privacy Protection Act
CPE	Common Platform Enumeration
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
CSP	Cloud Service Provider

ACRONYM	SPELLED OUT
CSR	Certificate Signing Request
CSRF	Cross-Site Request Forgery
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CYOD	Choose Your Own Device
DAC	Discretionary Access Control
DAST	Dynamic Application Security Testing
DDoS	Distributed Denial of Service
DEP	Data Execution Prevention
DLP	Data Loss Prevention
DNP3	Distributed Network Protocol 3
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoH	DNS over HTTPS
DoS	Denial of Service
DRM	Digital Rights Management
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm
EAP	Extensible Authentication Protocol
ECB	Electronic Codebook
ECDH	Elliptic-Curve Diffie-Hellman
ECDSA	Elliptic-Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
ERP	Enterprise Resource Planning
ESB	Enterprise Service Bus
FIM	File Integrity Monitoring
FPGA	Field-Programmable Gate Array
FTK	Forensic Toolkit
GCM	Galois/Counter Mode
GDPR	General Data Protection Regulation
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HMAC	Hash-based Message Authentication Code
HOTP	HMAC-based One-Time Password
HSM	Hardware Security Module
HSTS	HTTP Strict Transport Security
HTML	Hypertext Markup Language

ACRONYM	SPELLED OUT
HTTP	Hypertext Transfer Protocol
HUMINT	Human Intelligence
HVAC	Heating, Ventilation, and Air Conditioning
IaaS	Infrastructure as a Service
IAST	Interactive Application Security Testing
ICS	Industrial Control System
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISA	Interconnection Security Agreement
ISAC	Information Sharing Analysis Center
ISO	International Organization for Standardization
ISP	Internet Service Provider
JSON	JavaScript Object Notation
JWT	JSON Web Token
KVM	Keyboard, Video, and Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MD	Message Digest
MFA	Multifactor Authentication
MOU	Memorandum of Understanding
MSA	Master Service Agreement
MTBF	Mean Time Between Failure
MTTR	Mean Time to Recovery
NAC	Network Access Control
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
NFC	Near Field Communication
NGFW	Next Generation Firewall
NIC	Network Interface Controller
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology
NX	No Execute
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OFB	Output Feedback
OS	Operating System
OSINT	Open-Source Intelligence
OTP	One-Time Password
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PBKDF2	Password-Based Key Derivation Function 2
PBX	Private Branch Exchange
PCAP	Packet Capture
PCI DSS	Payment Card Industry Data Security Standard
PGP	Pretty Good Privacy
PII	Personal Identifiable Information

ACRONYM	SPELLED OUT
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PSK	Pre-Shared Key
QoS	Quality of Service
RA	Registration Authority
RACE	Research and Development in Advanced Communications Technologies in Europe
RADIUS	Remote Authentication Dial-in User Server
RAID	Redundant Array of Inexpensive Disks
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RF	Radio Frequency
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
ROI	Return on Investment
RPO	Recovery Point Objective
RSA	Rivest, Shamir, and Adleman
RTO	Recovery Time Objective
RTU	Remote Terminal Unit
S/MIME	Secure/Multipurpose Internet Mail Extensions
SaaS	Software as a Service
SAE	Simultaneous Authentication of Equals
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SASE	Secure Access Service Edge
SAST	Static Application Security Testing
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SDN	Software-Defined Networking
SDR	Software-Defined Radio
SD-WAN	Software-Defined Wide Area Network
SEAndroid	Security Enhanced Android
SED	Self-Encrypting Drive
SELinux	Security Enhanced Linux
SFTP	SSH File Transfer Protocol
SHA	Secure Hashing Algorithm
SIEM	Security Information Event Management
SLA	Service-Level Agreement
SLE	Single Loss Expectancy
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SOA	Start of Authority
SOAP	Simple Object Access Protocol
SOAR	Security Orchestration, Automation, and Response
SoC	System-on-Chip
SPAN	Switched Port Analyzer
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
STAR	Security Trust Assurance and Risk
TACACS	Terminal Access Controller Access Control System

ACRONYM	SPELLED OUT
TAP	Test Access Points
TCO	Total Cost of Ownership
TLS	Transport Layer Security
TOTP	Time-Based One-Time Password
TPM	Trusted Platform Module
UEBA	User and Entity Behavior Analytics
UEFI	Unified Extensible Firmware Interface
UTM	Unified Threat Management
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNET	Virtual Network
VNET	Virtual Network
VoIP	Voice over Internet Protocol
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAF	Web Application Firewall
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WPA	WiFi Protected Access
WS	Web Services
XCCDF	Extensible Configuration Checklist Description Format
XML	Extensible Markup Language
XN	Execute Never
XSS	Cross-Site Scripting

CASP+ Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the CASP+ exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

EQUIPMENT

- Laptops
- Basic server hardware (email server/ Active Directory server, trusted OS)
- Tokens
- Mobile devices (Android and iOS)
- Switches (managed switch)—IPv6 capable
- Gateway/router—IPv6 capable (wired/wireless)
- Firewall
- VoIP
- Proxy server
- Load balancer
- NIPS
- HSM
- Access points
- Crypto cards
- Smart cards
- Smart card reader
- Biometric devices
- Arduino/Raspberry Pi
- SCADA system: RTUs and PLCs

SPARE HARDWARE

- Keyboards
- Cables
- NICs
- Power supplies
- Removable media
- High-power graphics card

TOOLS

- Spectrum analyzer
- Antennas
- RF hacking hardware/SDR
- RSA token
- KVM switch

SOFTWARE

- Virtualized appliances (firewall, IPS, SIEM solution, RSA authentication, asterisk PBX)
- Windows
- Linux distros
- VMware Player/VirtualBox
- Vulnerability assessment tools
- SSH and Telnet utilities
- Threat modeling tool
- IPS/IDS, HIPS
- WIPS
- Forensic tools
- Certificate authority
- Kali and all Kali tool sets
- Remediation software
- GNS and associated firmware
- Log analysis tools
- APIs
- ELK Stack
- Graylog
- Python 3+
- Security Onion tools
- Metasploitable 2

OTHER

- Sample logs
- Sample network traffic (packet capture)
- Sample organizational structure
- Sample network documentation
- Broadband Internet connection
- 4G/5G and/or hotspot
- Computer and mobile peripheral devices
- Cloud services
- Visio/Excel
- Open Office

CompTIA