CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives

EXAM NUMBER: CAS-003

CompTIA

About the Exam

The CompTIA Advanced Security Practitioner (CASP+) CAS-003 certification is a vendor-neutral credential. The CASP+ exam is an internationally targeted validation of advanced-level security skills and knowledge. The CASP+ exam will certify the successful candidate has the technical knowledge and skills required to:

- **Conceptualize, engineer, integrate and implement secure solutions across complex environments to support a resilient enterprise**
- **Apply critical thinking and judgment across a broad spectrum of security disciplines to propose, implement and advocate sustainable security solutions that map to organizational strategies, balance security requirements with business/regulatory requirements, analyze risk impact and respond to security incidents**

The CASP+ certification is aimed at IT security professionals who have:

- **A minimum of ten years of experience in IT administration, including at least five years of hands-on technical security experience**
- **The following recommended prerequisites: CompTIA Network+, Security+, CySA+ or equivalent experience**

EXAM ACCREDITATION

The CASP+ certification 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.

**Candidates should have basic knowledge of vendor-specific tools and technologies, as this knowledge may be required for the CASP+ certification exam. CompTIA has included a sample list of hardware and software at the end of this document 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.

TEST DETAILS

Required exam	CAS-003
Number of questions	Maximum of 90
Types of questions	Multiple choice and performance-based
Length of test	165 minutes
Recommended experience	Ten years of experience in IT administration, including at least five years of hands-on technical security experience
Passing score	Pass/Fail only. No scaled score.

EXAM OBJECTIVES (DOMAINS)

The table below lists the domain areas measured by this examination and the approximate extent to which they are represented in the examination:

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Risk Management	19%
2.0 Enterprise Security Architecture	25%
3.0 Enterprise Security Operations	20%
4.0 Technical Integration of Enterprise Security	23%
5.0 Research, Development and Collaboration	13%
Total	**100%**

1.0 Risk Management

1.1 Summarize business and industry influences and associated security risks.

- **Risk management of new products, new technologies and user behaviors**
- **New or changing business models/strategies**
  - Partnerships
  - Outsourcing
  - Cloud
  - Acquisition/merger – divestiture/demerger
    - Data ownership
    - Data reclassification
- **Security concerns of integrating diverse industries**
  - Rules
  - Policies
  - Regulations
    - Export controls
    - Legal requirements
  - Geography
    - Data sovereignty
    - Jurisdictions
- **Internal and external influences**
  - Competitors
  - Auditors/audit findings
  - Regulatory entities
  - Internal and external client requirements
  - Top-level management
- **Impact of de-perimeterization (e.g., constantly changing network boundary)**
  - Telecommuting
  - Cloud
  - Mobile
  - BYOD
  - Outsourcing
  - Ensuring third-party providers have requisite levels of information security

1.2 Compare and contrast security, privacy policies and procedures based on organizational requirements.

- **Policy and process life cycle management**
  - New business
  - New technologies
  - Environmental changes
  - Regulatory requirements
  - Emerging risks
- **Support legal compliance and advocacy by partnering with human resources, legal, management and other entities**
- **Understand common business documents to support security**
  - Risk assessment (RA)
  - Business impact analysis (BIA)
  - Interoperability agreement (IA)
  - Interconnection security agreement (ISA)
  - Memorandum of understanding (MOU)
  - Service-level agreement (SLA)
  - Operating-level agreement (OLA)
  - Non-disclosure agreement (NDA)
  - Business partnership agreement (BPA)
  - Master service agreement (MSA)
- **Research security requirements for contracts**
  - Request for proposal (RFP)
  - Request for quote (RFQ)
  - Request for information (RFI)
- **Understand general privacy principles for sensitive information**
- **Support the development of policies containing standard security practices**
  - Separation of duties
  - Job rotation
  - Mandatory vacation
  - Least privilege
  - Incident response
  - Forensic tasks
  - Employment and termination procedures
  - Continuous monitoring
  - Training and awareness for users
  - Auditing requirements and frequency
  - Information classification

1.3 Given a scenario, execute risk mitigation strategies and controls.

- **Categorize data types by impact levels based on CIA**
- **Incorporate stakeholder input into CIA impact-level decisions**
- **Determine minimum-required security controls based on aggregate score**
- **Select and implement controls based on CIA requirements and organizational policies**
- **Extreme scenario planning/ worst-case scenario**
- **Conduct system-specific risk analysis**
- **Make risk determination based upon known metrics**
  - Magnitude of impact based on ALE and SLE
  - Likelihood of threat
    - Motivation
    - Source
    - ARO
    - Trend analysis
  - Return on investment (ROI)
  - Total cost of ownership
- **Translate technical risks in business terms**
- **Recommend which strategy should be applied based on risk appetite**
  - Avoid
  - Transfer
  - Mitigate
  - Accept
- **Risk management processes**
  - Exemptions
  - Deterrence
  - Inherent
  - Residual
- **Continuous improvement/monitoring**
- **Business continuity planning**
  - RTO
  - RPO
  - MTTR
  - MTBF
- **IT governance**
  - Adherence to risk management frameworks
- **Enterprise resilience**

1.4 Analyze risk metric scenarios to secure the enterprise.

- **Review effectiveness of existing security controls**
  - Gap analysis
  - Lessons learned
  - After-action reports
- **Reverse engineer/deconstruct existing solutions**
- **Creation, collection and analysis of metrics**
  - KPIs
  - KRIs
- **Prototype and test multiple solutions**
- **Create benchmarks and compare to baselines**
- **Analyze and interpret trend data to anticipate cyber defense needs**
- **Analyze security solution metrics and attributes to ensure they meet business needs**
  - Performance
  - Latency
  - Scalability
  - Capability
  - Usability
  - Maintainability
  - Availability
  - Recoverability
  - ROI
  - TCO
- **Use judgment to solve problems where the most secure solution is not feasible**

2.0 Enterprise Security Architecture

2.1 Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

- **Physical and virtual network and security devices**
  - UTM
  - IDS/IPS
  - NIDS/NIPS
  - INE
  - NAC
  - SIEM
  - Switch
  - Firewall
  - Wireless controller
  - Router
  - Proxy
  - Load balancer
  - HSM
  - MicroSD HSM
- **Application and protocol-aware technologies**
  - WAF
  - Firewall
  - Passive vulnerability scanners
  - DAM
- **Advanced network design (wired/wireless)**
  - Remote access
    - VPN
      - IPSec
      - SSL/TLS
    - SSH
    - RDP
    - VNC
    - VDI
    - Reverse proxy
  - IPv4 and IPv6 transitional technologies
  - Network authentication methods
  - 802.1x
  - Mesh networks
  - Placement of fixed/mobile devices
  - Placement of hardware and applications
- **Complex network security solutions for data flow**
  - DLP
  - Deep packet inspection
  - Data flow enforcement
  - Network flow (S/flow)
  - Data flow diagram
- **Secure configuration and baselining of networking and security components**
- **Software-defined networking**
- **Network management and monitoring tools**
  - Alert definitions and rule writing
  - Tuning alert thresholds
  - Alert fatigue
- **Advanced configuration of routers, switches and other network devices**
  - Transport security
  - Trunking security
  - Port security
  - Route protection
  - DDoS protection
  - Remotely triggered sinkhole (previously known as remotely triggered black hole)
- **Security zones**
  - Screened subnet (previously known as demilitarized zone)
  - Separation of critical assets
  - Network segmentation
- **Network access control**
  - Quarantine/remediation
  - Persistent/volatile or non-persistent agent
  - Agent vs. agentless
- **Network-enabled devices**
  - System on a chip (SoC)
  - Building/home automation systems
  - IP video
  - HVAC controllers
  - Sensors
  - Physical access control systems
  - A/V systems
  - Scientific/industrial equipment
- **Critical infrastructure**
  - Supervisory control and data acquisition (SCADA)
  - Industrial control systems (ICS)

2.2 Analyze a scenario to integrate security controls for host devices to meet security requirements.

- **Trusted OS (e.g., how and when to use it)**
  - SELinux
  - SEAndroid
  - TrustedSolaris
  - Least functionality
- **Endpoint security software**
  - Anti-malware
  - Antivirus
  - Anti-spyware
  - Spam filters
  - Patch management
  - HIPS/HIDS
  - Data loss prevention
  - Host-based firewalls
  - Log monitoring
  - Endpoint detection response
- **Host hardening**
  - Standard operating environment/ configuration baselining
    - Application allow list and deny list
  - Security/group policy implementation
  - Command shell restrictions
  - Patch management
    - Manual
    - Automated
      - Scripting and replication
  - Configuring dedicated interfaces
    - Out-of-band management
    - ACLs
    - Management interface
    - Data interface
  - External I/O restrictions
    - USB
    - Wireless
      - Bluetooth
      - NFC
      - IrDA
      - RF
      - 802.11
      - RFID
    - Drive mounting
    - Drive mapping
    - Webcam
    - Recording mic
    - Audio output
    - SD port
    - HDMI port
  - File and disk encryption
  - Firmware updates
- **Boot loader protections**
  - Secure boot
  - Measured launch
  - Integrity measurement architecture
  - BIOS/UEFI
  - Attestation services
  - TPM
- **Vulnerabilities associated with hardware**
- **Terminal services/application delivery services**

2.3 Analyze a scenario to integrate security controls for mobile and small form factor devices to meet security requirements.

- **Enterprise mobility management**
  - Containerization
  - Configuration profiles and payloads
  - Personally owned, corporate-enabled
  - Application wrapping
  - Remote assistance access
    - VNC
    - Screen mirroring
  - Application, content and data management
  - Over-the-air updates (software/firmware)
  - Remote wiping
  - SCEP
  - BYOD
  - COPE
  - VPN
  - Application permissions
  - Side loading
  - Unsigned apps/system apps
  - Context-aware management
    - Geolocation/geofencing
    - User behavior
    - Security restrictions
    - Time-based restrictions
- **Security implications/privacy concerns**
  - Data storage
    - Non-removable storage
    - Removable storage
    - Cloud storage
    - Transfer/backup data to uncontrolled storage
    - USB OTG
  - Device loss/theft
  - Hardware anti-tamper
    - eFuse
  - TPM
  - Rooting/jailbreaking
  - Push notification services
  - Geotagging
  - Encrypted instant messaging apps
  - Tokenization
  - OEM/carrier Android fragmentation
  - Mobile payment
    - NFC-enabled
    - Inductance-enabled
    - Mobile wallet
    - Peripheral-enabled payments (credit card reader)
  - Tethering
    - USB
    - Spectrum management
    - Bluetooth 3.0 vs. 4.1
  - Authentication
    - Swipe pattern
    - Gesture
    - Pin code
    - Biometric
      - Facial
      - Fingerprint
      - Iris scan
  - Malware
  - Unauthorized domain bridging
  - Baseband radio/SOC
  - Augmented reality
  - SMS/MMS/messaging
- **Wearable technology**
  - Devices
    - Cameras
    - Watches
    - Fitness devices
    - Glasses
    - Medical sensors/devices
    - Headsets
  - Security implications
    - Unauthorized remote activation/deactivation of devices or features
    - Encrypted and unencrypted communication concerns
    - Physical reconnaissance
    - Personal data theft
    - Health privacy
    - Digital forensics of collected data

2.4 Given software vulnerability scenarios, select appropriate security controls.

- **Application security design considerations**
  - Secure: by design, by default, by deployment
- **Specific application issues**
  - Unsecure direct object references
  - XSS
  - Cross-site request forgery (CSRF)
  - Click-jacking
  - Session management
  - Input validation
  - SQL injection
  - Improper error and exception handling
  - Privilege escalation
  - Improper storage of sensitive data
  - Fuzzing/fault injection
  - Secure cookie storage and transmission
  - Buffer overflow
  - Memory leaks
  - Integer overflows
  - Race conditions
    - Time of check
    - Time of use
  - Resource exhaustion
  - Geotagging
  - Data remnants
  - Use of third-party libraries
  - Code reuse
- **Application sandboxing**
- **Secure encrypted enclaves**
- **Database activity monitor**
- **Web application firewalls**
- **Client-side processing vs. server-side processing**
  - JSON/REST
  - Browser extensions
    - ActiveX
    - Java applets
  - HTML5
  - AJAX
  - SOAP
  - State management
  - JavaScript
- **Operating system vulnerabilities**
- **Firmware vulnerabilities**

3.0 Enterprise Security Operations

3.1 Given a scenario, conduct a security assessment using the appropriate methods.

- **Methods**
  - Malware sandboxing
  - Memory dumping, runtime debugging
  - Reconnaissance
  - Fingerprinting
  - Code review
  - Social engineering
  - Pivoting
  - Open source intelligence
    - Social media
    - Whois
    - Routing tables
    - DNS records
    - Search engines
- **Types**
  - Penetration testing
    - Unknown environment
    - Known environment
    - Partially known environment
  - Vulnerability assessment
  - Self-assessment
    - Tabletop exercises
    - Internal and external audits
  - Color team exercises
    - Red team
    - Blue team
    - White team

3.2 Analyze a scenario or output, and select the appropriate tool for a security assessment.

- **Network tool types**
  - Port scanners
  - Vulnerability scanners
  - Protocol analyzer
    - Wired
    - Wireless
  - SCAP scanner
  - Network enumerator
  - Fuzzer
  - HTTP interceptor
  - Exploitation tools/frameworks
  - Visualization tools
  - Log reduction and analysis tools
- **Host tool types**
  - Password cracker
  - Vulnerability scanner
  - Command line tools
  - Local exploitation tools/frameworks
  - SCAP tool
  - File integrity monitoring
  - Log analysis tools
  - Antivirus
  - Reverse engineering tools
- **Physical security tools**
  - Lock picks
  - RFID tools
  - IR camera

3.3 Given a scenario, implement incident response and recovery procedures.

- **E-discovery**
  - Electronic inventory and asset control
  - Data retention policies
  - Data recovery and storage
  - Data ownership
  - Data handling
  - Legal holds
- **Data breach**
  - Detection and collection
    - Data analytics
  - Mitigation
    - Minimize
    - Isolate
  - Recovery/reconstitution
  - Response
  - Disclosure
- **Facilitate incident detection and response**
  - Hunt teaming
  - Heuristics/behavioral analytics
  - Establish and review system, audit and security logs
- **Incident and emergency response**
  - Chain of custody
  - Forensic analysis of compromised system
  - Continuity of operations
  - Disaster recovery
  - Incident response team
  - Order of volatility
- **Incident response support tools**
  - dd
  - tcpdump
  - nbtstat
  - netstat
  - nc (Netcat)
  - memdump
  - tshark
  - foremost
- **Severity of incident or breach**
  - Scope
  - Impact
  - Cost
  - Downtime
  - Legal ramifications
- **Post-incident response**
  - Root-cause analysis
  - Lessons learned
  - After-action report

4.0 Technical Integration of Enterprise Security

4.1 Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

- **Adapt data flow security to meet changing business needs**
- **Standards**
  - Open standards
  - Adherence to standards
  - Competing standards
  - Lack of standards
  - De facto standards
- **Interoperability issues**
  - Legacy systems and software/current systems
  - Application requirements
  - Software types
    - In-house developed
    - Commercial
    - Tailored commercial
    - Open source
  - Standard data formats
  - Protocols and APIs
- **Resilience issues**
  - Use of heterogeneous components
  - Course of action automation/orchestration
  - Distribution of critical assets
  - Persistence and non-persistence of data
  - Redundancy/high availability
  - Assumed likelihood of attack
- **Data security considerations**
  - Data remnants
  - Data aggregation
  - Data isolation
  - Data ownership
  - Data sovereignty
  - Data volume
- **Resources provisioning and deprovisioning**
  - Users
  - Servers
  - Virtual devices
  - Applications
  - Data remnants
- **Design considerations during mergers, acquisitions and demergers/divestitures**
- **Network secure segmentation and delegation**
- **Logical deployment diagram and corresponding physical deployment diagram of all relevant devices**
- **Security and privacy considerations of storage integration**
- **Security implications of integrating enterprise applications**
  - CRM
  - ERP
  - CMDB
  - CMS
  - Integration enablers
    - Directory services
    - DNS
    - SOA
    - ESB

4.2 Given a scenario, integrate cloud and virtualization technologies into a secure enterprise architecture.

- **Technical deployment models (outsourcing/insourcing/ managed services/partnership)**
  - Cloud and virtualization considerations and hosting options
    - Public
    - Private
    - Hybrid
    - Community
    - Multi-tenancy
    - Single tenancy
  - On-premise vs. hosted
  - Cloud service models
    - SaaS
    - IaaS
    - PaaS
- **Security advantages and disadvantages of virtualization**
  - Type 1 vs. Type 2 hypervisors
  - Container-based
  - vTPM
  - Hyperconverged infrastructure
  - Virtual desktop infrastructure
  - Secure enclaves and volumes
- **Cloud augmented security services**
  - Anti-malware
  - Vulnerability scanning
  - Sandboxing
  - Content filtering
  - Cloud security broker
  - Security as a service
  - Managed security service providers
- **Vulnerabilities associated with comingling of hosts with different security requirements**
  - VMEscape
  - Privilege elevation
  - Live VM migration
  - Data remnants
- **Data security considerations**
  - Vulnerabilities associated with a single server hosting multiple data types
  - Vulnerabilities associated with a single platform hosting multiple data types/owners on multiple virtual machines
- **Resources provisioning and deprovisioning**
  - Virtual devices
  - Data remnants

4.3 Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

- **Authentication**
  - Certificate-based authentication
  - Single sign-on
  - 802.1x
  - Context-aware authentication
  - Push-based authentication
- **Authorization**
  - OAuth
  - XACML
  - SPML
- **Attestation**
- **Identity proofing**
- **Identity propagation**
- **Federation**
  - SAML
  - OpenID
  - Shibboleth
  - WAYF
- **Trust models**
  - RADIUS configurations
  - LDAP
  - AD

4.4 Given a scenario, implement cryptographic techniques.

- **Techniques**
  - Key stretching
  - Hashing
  - Digital signature
  - Message authentication
  - Code signing
  - Pseudo-random number generation
  - Perfect forward secrecy
  - Data-in-transit encryption
  - Data-in-memory/processing
  - Data-at-rest encryption
    - Disk
    - Block
    - File
    - Record
  - Steganography
- **Implementations**
  - Crypto modules
  - Crypto processors
  - Cryptographic service providers
  - DRM
  - Watermarking
  - GPG
  - SSL/TLS
  - SSH
  - S/MIME
  - Cryptographic applications and proper/improper implementations
    - Strength
    - Performance
    - Feasibility to implement
    - Interoperability
  - Stream vs. block
  - PKI
    - Wild card
    - OCSP vs. CRL
    - Issuance to entities
    - Key escrow
    - Certificate
    - Tokens
    - Stapling
    - Pinning
  - Cryptocurrency/blockchain
  - Mobile device encryption considerations
  - Elliptic curve cryptography
    - P-256 vs. P-384 vs. P521

4.5 Given a scenario, select the appropriate control to secure communications and collaboration solutions.

- **Remote access**
  - Resource and services
  - Desktop and application sharing
  - Remote assistance
- **Unified collaboration tools**
  - Conferencing
    - Web
    - Video
    - Audio
  - Storage and document collaboration tools
  - Unified communication
  - Instant messaging
  - Presence
  - Email
  - Telephony and VoIP integration
  - Collaboration sites
    - Social media
    - Cloud-based

5.0 Research, Development and Collaboration

5.1 Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.

- **Perform ongoing research**
  - Best practices
  - New technologies, security systems and services
  - Technology evolution (e.g., RFCs, ISO)
- **Threat intelligence**
  - Latest attacks
  - Knowledge of current vulnerabilities and threats
  - Zero-day mitigation controls and remediation
  - Threat model
- **Research security implications of emerging business tools**
  - Evolving social media platforms
  - Integration within the business
  - Big Data
  - AI/machine learning
- **Global IA industry/community**
  - Computer emergency response team (CERT)
  - Conventions/conferences
  - Research consultants/vendors
  - Threat actor activities
  - Emerging threat sources

5.2 Given a scenario, implement security activities across the technology life cycle.

- **Systems development life cycle**
  - Requirements
  - Acquisition
  - Test and evaluation
  - Commissioning/decommissioning
  - Operational activities
    - Monitoring
    - Maintenance
    - Configuration and change management
  - Asset disposal
  - Asset/object reuse
- **Software development life cycle**
  - Application security frameworks
  - Software assurance
    - Standard libraries
    - Industry-accepted approaches
    - Web services security (WS-security)
  - Forbidden coding techniques
  - NX/XN bit use
  - ASLR use
  - Code quality
  - Code analyzers
    - Fuzzer
    - Static
    - Dynamic
  - Development approaches
    - DevOps
    - Security implications of agile, waterfall and spiral software development methodologies
    - Continuous integration
    - Versioning
  - Secure coding standards
  - Documentation
    - Security requirements traceability matrix (SRTM)
    - Requirements definition
    - System design document
    - Testing plans
  - Validation and acceptance testing
    - Regression
    - User acceptance testing
    - Unit testing
    - Integration testing
    - Peer review
- **Adapt solutions to address:**
  - Emerging threats
  - Disruptive technologies
  - Security trends
- **Asset management (inventory control)**

5.3 Explain the importance of interaction across diverse business units to achieve security goals.

- **Interpreting security requirements and goals to communicate with stakeholders from other disciplines**
  - Sales staff
  - Programmer
  - Database administrator
  - Network administrator
  - Management/executive management
  - Financial
  - Human resources
  - Emergency response team
  - Facilities manager
  - Physical security manager
  - Legal counsel
- **Provide objective guidance and impartial recommendations to staff and senior management on security processes and controls**
- **Establish effective collaboration within teams to implement secure solutions**
- **Governance, risk and compliance committee**

CASP+ Acronyms

The following is a list of acronyms that appear on the CASP+ 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
AAA	Authentication, Authorization and Accounting
AAR	After Action Report
ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
AH	Authentication Header
AJAX	Asynchronous JavaScript and XML
ALE	Annualized Loss Expectancy
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
AUP	Acceptable Use Policy
AV	Antivirus
B2B	Business-to-Business
BCP	Business Continuity Planning
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
BPA	Business Partnership Agreement
BPM	Business Process Management
BYOD	Bring Your Own Device
CA	Certificate Authority
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CASB	Cloud Access Security Broker
CBC	Cipher Block Chaining
CCMP	Counter-Mode/CBC-Mac Protocol
CCTV	Closed-Circuit Television
CERT	Computer Emergency Response Team
CFB	Cipher Feedback
CHAP	Challenge Handshake Authentication Protocol
CIA	Confidentiality, Integrity and Availability
CIFS	Common Internet File System
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CLI	Command Line Interface
CMDB	Configuration Management Database
CMS	Content Management System
COOP	Continuity of Operations
COPE	Corporate Owned, Personally Enabled
COTS	Commercial Off-the-Shelf
CRC	Cyclical Redundancy Check
CredSSP	Credential Security Support Provider
CRL	Certification Revocation List
CRM	Customer Resource Management
CSP	Cloud Service Provider
CSP	Cryptographic Service Provider
CSRF	Cross-Site Request Forgery
CTR	Counter Mode
CVE	Collaborative Virtual Environment
CYOD	Choose Your Own Device
DAC	Discretionary Access Control
DAM	Database Activity Monitoring
DAR	Data at Rest
DDoS	Distributed Denial of Service
DEP	Data Execution Prevention
DES	Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DKIM	Domain Keys Identified Mail
DLL	Dynamic Link Library
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name Service
DOM	Document Object Model
DoS	Denial of Service
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm

ACRONYM	SPELLED OUT
EAP	Extensible Authentication Protocol
ECB	Event Control Block
ECC	Elliptic Curve Cryptography
EDR	Endpoint Detection Response
EFS	Encrypted File System
EMI	Electromagnetic Interference
ERP	Enterprise Resource Planning
ESA	Enterprise Security Architecture
ESB	Enterprise Service Bus
ESP	Encapsulated Security Payload
EV	Extended Validation (Certificate)
FDE	Full Disk Encryption
FIM	File Integrity Monitoring
FTP	File Transfer Protocol
GPG	GNU Privacy Guard
GPO	Group Policy Object
GPU	Graphic Processing Unit
GRC	Governance, Risk and Compliance
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HDD	Hard Disk Drive
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HMAC	Hashed Message Authentication Code
HOTP	HMAC-based One-Time Password
HSM	Hardware Security Module
HSTS	HTTP Strict Transport Security
HVAC	Heating, Ventilation and Air Conditioning
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDE	Integrated Development Environment
IdM	Identity Management
IdP	Identity Provider
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP	Internet Message Access Protocol
INE	Inline Network Encryptor
IOC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPMI	Internet Protocol Multicast Initiative
IPS	Intrusion Prevention Systems
IPSec	Internet Protocol Security

ACRONYM	SPELLED OUT
IR	Incident Response
IRC	Internet Relay Chat
IS-IS	Intermediate System to Intermediate System
ISA	Interconnection Security Agreement
ISAC	Information Sharing Analysis Center
ISMS	Information Security Management System
ISP	Internet Service Provider
IV	Initialization Vector
JSON	JavaScript Object Notation
KDC	Key Distribution Center
KPI	Key Performance Indicator
KRI	Key Risk Indicator
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
LTE	Long-Term Evolution
LUN	Logical Unit Number
MAC	Mandatory Access Control
MAC	Media Access Control
MAC	Message Authentication Code
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MBR	Master Boot Record
MD5	Message Digest 5
MDM	Mobile Device Management
MEAP	Mobile Enterprise Application Platform
MFA	Multifactor Authentication
MFD	Multifunction Device
MITM	Man in the Middle
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
MSA	Master Service Agreement
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSS	Managed Security Service
MSSP	Managed Security Service Provider
MTA	Message Transfer Agent
MTBF	Mean Time Between Failure
MTD	Maximum Tolerable Downtime
MTP	Media Transfer Protocol
MTTR	Mean Time to Recovery
MTU	Maximum Transmission Unit
NAC	Network Access Control

ACRONYM	SPELLED OUT
NAS	Network Attached Storage
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
NFC	Near Field Communication
NFS	Network File System
NGFW	Next Generation Firewall
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology
NLA	Network-Level Authentication
NOS	Network Operating System
NSP	Network Service Provider
NTFS	New Technology File System
NTLM	New Technology LAN Manager
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OLA	Operating-Level Agreement
OOB	Out-of-Band
OS	Operating System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OTP	One-Time Password
OVAL	Open Vulnerability Assessment Language
OWASP	Open Web Application Security Project
P2P	Peer-to-Peer
PaaS	Platform as a Service
PAP	Password Authentication Protocol
PAT	Port Address Translation
PBKDF2	Password-Based Key Derivation Function 2
PBX	Private Branch Exchange
PCI-DSS	Payment Card Industry Data Security Standard
PDP	Policy Distribution Point
PEAP	Protected Extensible Authentication Protocol
PEP	Policy Enforcement Point
PFS	Perfect Forward Secrecy
PGP	Pretty Good Privacy
PII	Personal Identifiable Information
PIP	Policy Information Point
PIR	Post Incident Report
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
POC	Proof of Concept
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-Shared Key
QA	Quality Assurance

ACRONYM	SPELLED OUT
QoS	Quality of Service
R&D	Research and Development
RA	Recovery Agent
RA	Registration Authority
RADIUS	Remote Authentication Dial-in User Server
RAID	Redundant Array of Inexpensive/Independent Disks
RAS	Remote Access Server
RBAC	Role-Based Access Control
RBAC	Rule-Based Access Control
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RFC	Request for Comments
RFI	Request for Information
RFID	Radio Frequency Identification
RFP	Request for Proposal
RFQ	Request for Quote
ROI	Return on Investment
RPO	Recovery Point Objective
RSA	Rivest, Shamir and Adleman
RTO	Recovery Time Objective
RTP	Real-time Transport Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SaaS	Software as a Service
SAML	Security Assertions Markup Language
SAN	Subject Alternative Name
SAN	Storage Area Network
SAS	Statement on Auditing Standards
SATCOM	Satellite Communications
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy
SCSI	Small Computer System Interface
SDL	Security Development Life Cycle
SDLC	Software Development Life Cycle
SED	Self-Encrypting Drive
SELinux	Security Enhanced Linux
SFTP	Secure File Transfer Protocol
SHA	Secure Hashing Algorithm
SIEM	Security Information Event Management
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service-Level Agreement
SLE	Single Loss Expectancy
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol

ACRONYM	SPELLED OUT
SNAT	Source Network Address Translation
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SOA	Start of Authority
SOA	Statement of Applicability
SOAP	Simple Object Access Protocol
SOC	Security Operations Center
SOC	Service Organization Controls
SOE	Standard Operating Environment
SOP	Standard Operating Procedure
SOW	Statement of Work
SOX	Sarbanes-Oxley Act of 2002
SP	Service Provider
SPIM	Spam over Internet Messaging
SPML	Service Provisioning Markup Language
SRTM	Security Requirements Traceability Matrix
SRTP	Secure Real-Time Protocol
SRV	Service Records
SSD	Solid State Drive
SSDLC	Security System Development Life Cycle
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
SSP	Storage Service Provider
TACACS	Terminal Access Controller Access Control System
TCO	Total Cost of Ownership
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOC/TOU	Time of Check/Time of Use
TOS	Type of Service
TOTP	Time-based One-Time Password
TPM	Trusted Platform Module
TSIG	Transaction Signature Interoperability Group
TTR	Time to Restore
UAC	User Access Control
UAT	User Acceptance Testing
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UPS	Uninterruptable Power Supply
URL	Universal Resource Locator
USB	Universal Serial Bus
UTM	Unified Threat Management
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VM	Virtual Machine

ACRONYM	SPELLED OUT
VMFS	VMware File System
VNC	Virtual Network Connection
VoIP	Voice over IP
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
vSAN	Virtual Storage Area Network
VTC	Video Teleconferencing
vTPM	Virtual Trusted Platform Module
WAF	Web Application Firewall
WAP	Wireless Access Point
WAYF	Where Are You From
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WMI	Windows Management Interface
WPA	Wireless Protected Access
WRT	Work Recovery Time
WSDL	Web Services Description Language
XACML	eXtensible Access Control Markup Language
XHR	XMLHttpRequest
XMPP	eXtensible Messaging and Presence Protocol
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 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
- Router – IPv6 capable (wired/wireless)
- Gateway
- Firewall
- VoIP
- Proxy server
- Load balancer
- NIPS
- HSM
- Access points
- Crypto-cards
- Smart cards
- Smart card reader
- Biometric devices
- Arduino/Raspberry Pi
- SCADA device

SPARE HARDWARE

- Keyboards
- Cables
- NICs
- Power supplies
- External USB flash drives

TOOLS

- Spectrum analyzer
- Antennas
- RF hacking hardware/SDR

SOFTWARE

- Virtualized appliances (firewall, IPS, SIEM solution, RSA authentication, Asterisk PBX)
- Windows
- Linux distros
- VMWare player/virtual box
- Vulnerability assessment tools
- SSH and Telnet utilities
- Threat modeling tool
- Host IPS
- Helix software
- Kali and all Kali toolsets
- Remediation software
- GNS and associated firmware
- Log analysis tools

OTHER

- Sample logs
- Sample network traffic (packet capture)
- Sample organizational structure
- Sample network documentation
- Broadband Internet connection
- 3G/4G and/or hotspot
- Computer and mobile peripheral devices

CompTIA