CompTIA Advanced Security Practitioner Certification Exam Objectives

EXAM NUMBER: CAS-002

CompTIA

About the Exam

The CompTIA Advanced Security Practitioner (CASP) CAS-002 certification is a vendor-neutral credential. The CASP exam is an internationally targeted validation of advanced-level security skills and knowledge. Candidates are encouraged to use this document to help prepare for the CASP exam, which measures necessary skills for IT security professionals. Successful candidates will have the knowledge required to:

- **Conceptualize, engineer, integrate and implement secure solutions across complex environments**
- **Apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement sustainable security solutions that map to organizational strategies**
- **Translate business needs into security requirements**
- **Analyze risk impact**
- **Respond to security incidents**

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

CASP is accredited by ANSI to show compliance with the ISO 17024 Standard and, as such, undergoes regular reviews and updates to the exam objectives.

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	CASP CAS-002
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	CASP CAS-002: 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 Enterprise Security	30%
2.0 Risk Management and Incident Response	20%
3.0 Research and Analysis	18%
4.0 Integration of Computing, Communications and Business Disciplines	16%
5.0 Technical Integration of Enterprise Components	16%
Total	**100%**

1.0 Enterprise Security

1.1 Given a scenario, select appropriate cryptographic concepts and techniques.

- **Techniques**
  - Key stretching
  - Hashing
  - Code signing
  - Pseudorandom number generation
  - Perfect forward secrecy
  - Transport encryption
  - Data-at-rest encryption
  - Digital signature
- **Concepts**
  - Entropy
  - Diffusion
  - Confusion
  - Non-repudiation
  - Confidentiality
  - Integrity
  - Chain of trust, root of trust
  - Cryptographic applications and proper/improper implementations
  - Advanced PKI concepts
    - Wild card
    - OCSP vs. CRL
    - Issuance to entities
    - Users
    - Systems
    - Applications
    - Key escrow
  - Steganography
  - Implications of cryptographic methods and design
    - Stream
    - Block
    - Modes
    - ECB
    - CBC
    - CFB
    - OFB
    - Known flaws/weaknesses
    - Strength vs. performance vs. feasibility to implement vs. interoperability
- **Implementations**
  - DRM
  - Watermarking
  - GPG
  - SSL
  - SSH
  - S/MIME

1.2 Explain the security implications associated with enterprise storage.

- **Storage types**
  - Virtual storage
  - Cloud storage
  - Data warehousing
  - Data archiving
  - NAS
  - SAN
  - vSAN
- **Storage protocols**
  - iSCSI
  - FCoE
  - NFS, CIFS
- **Secure storage management**
  - Multipath
  - Snapshots
  - Deduplication
  - Dynamic disk pools
  - LUN masking/mapping
  - HBA allocation
  - Offsite or multisite replication
  - Encryption
    - Disk
    - Block
    - File
    - Record
    - Port

CompTIA

1.3 Given a scenario, analyze network and security components, concepts and architectures.

- **Advanced network design (wired/wireless)**
  - Remote access
    - VPN
    - SSH
    - RDP
    - VNC
    - SSL
  - IPv6 and associated transitional technologies
  - Transport encryption
  - Network authentication methods
  - 802.1x
  - Mesh networks
- **Security devices**
  - UTM
  - NIPS
  - NIDS
  - INE
  - SIEM
  - HSM
  - Placement of devices
  - Application and protocol aware technologies
    - WAF
    - NextGen firewalls
    - IPS
    - Passive vulnerability scanners
    - DAM
- **Virtual networking and security components**
  - Switches
  - Firewalls
  - Wireless controllers
  - Routers
  - Proxies
- **Complex network security solutions for data flow**
  - SSL inspection
  - Network flow data
- **Secure configuration and baselining of networking and security components**
  - ACLs
  - Change monitoring
  - Configuration lockdown
  - Availability controls
- **Software-defined networking**
- **Cloud-managed networks**
- **Network management and monitoring tools**
- **Advanced configuration of routers, switches and other network devices**
  - Transport security
  - Trunking security
  - Route protection
- **Security zones**
  - Data flow enforcement
  - DMZ
  - Separation of critical assets
- **Network access control**
  - Quarantine/remediation
- **Operational and consumer network-enabled devices**
  - Building 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)**

1.4 Given a scenario, select and troubleshoot security controls for hosts.

- **Trusted OS (e.g., how and when to use it)**
- **Endpoint security software**
  - Anti-malware
  - Antivirus
  - Anti-spyware
  - Spam filters
  - Patch management
  - HIPS/HIDS
  - Data loss prevention
  - Host-based firewalls
  - Log monitoring
- **Host hardening**
  - Standard operating environment/ configuration baselining
    - Application whitelisting and blacklisting
  - Security/group policy implementation
  - Command shell restrictions
  - Patch management
  - Configuring dedicated interfaces
    - Out-of-band NICs
    - ACLs
    - Management interface
    - Data interface
  - Peripheral restrictions
    - USB
    - Bluetooth
    - Firewire
  - Full disk encryption
- **Security advantages and disadvantages of virtualizing servers**
  - Type I
  - Type II
  - Container-based
- **Cloud augmented security services**
  - Hash matching
    - Antivirus
    - Anti-spam
    - Vulnerability scanning
  - Sandboxing
    - Content filtering
- **Boot loader protections**
  - Secure boot
  - Measured launch
  - Integrity Measurement Architecture (IMA)
  - BIOS/UEFI
- **Vulnerabilities associated with co-mingling of hosts with different security requirements**
  - VM escape
  - Privilege elevation
  - Live VM migration
  - Data remnants
- **Virtual Desktop Infrastructure (VDI)**
- **Terminal services/application delivery services**
- **TPM**
- **VTPM**
- **HSM**

1.5 Differentiate application vulnerabilities and select appropriate security controls.

- **Web application security design considerations**
  - Secure: by design, by default, by deployment
- **Specific application issues**
  - 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
  - Geo-tagging
  - Data remnants
- **Application sandboxing**
- **Application security frameworks**
  - Standard libraries
  - Industry-accepted approaches
  - Web services security (WS-security)
- **Secure coding standards**
- **Database Activity Monitor (DAM)**
- **Web Application Firewalls (WAF)**
- **Client-side processing vs. server-side processing**
  - JSON/REST
  - Browser extensions
    - ActiveX
    - Java Applets
    - Flash
  - HTML5
  - AJAX
  - SOAP
  - State management
  - JavaScript

2.0 Risk Management and Incident Response

2.1 Interpret business and industry influences and explain associated security risks.

- **Risk management of new products, new technologies and user behaviors**
- **New or changing business models/strategies**
  - Partnerships
  - Outsourcing
  - Cloud
  - Merger and demerger/divestiture
- **Security concerns of integrating diverse industries**
  - Rules
  - Policies
  - Regulations
  - Geography
- **Ensuring third-party providers have requisite levels of information security**
- **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
  - BYOD
  - Outsourcing

2.2 Given a scenario, execute risk mitigation planning, strategies and controls.

- **Classify information types into levels of CIA based on organization/industry**
- **Incorporate stakeholder input into CIA decisions**
- **Implement technical controls based on CIA requirements and policies of the organization**
- **Determine aggregate score of CIA**
- **Extreme scenario planning/ worst case scenario**
- **Determine minimum required security controls based on aggregate score**
- **Conduct system specific risk analysis**
- **Make risk determination**
  - Magnitude of impact
    - ALE
    - SLE
  - Likelihood of threat
    - Motivation
    - Source
    - ARO
    - Trend analysis
  - Return On Investment (ROI)
  - Total cost of ownership
- **Recommend which strategy should be applied based on risk appetite**
  - Avoid
  - Transfer
  - Mitigate
  - Accept
- **Risk management processes**
  - Exemptions
  - Deterrance
  - Inherent
  - Residual
- **Enterprise security architecture frameworks**
- **Continuous improvement/monitoring**
- **Business continuity planning**
- **IT governance**

CompTIA

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

- **Policy development and updates in light of new business, technology, risks and environment changes**
- **Process/procedure development and updates in light of policy, environment and business changes**
- **Support legal compliance and advocacy by partnering with HR, legal, management and other entities**
- **Use common business documents to support security**
  - Risk assessment (RA)/ Statement Of Applicability (SOA)
  - 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)
- **Use general privacy principles for sensitive information (PII)**
- **Support the development of policies that contain**
  - 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

2.4 Given a scenario, conduct 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
- **Design systems to facilitate incident response**
  - Internal and external violations
    - Privacy policy violations
    - Criminal actions
    - Insider threat
    - Non-malicious threats/ misconfigurations
  - Establish and review system, audit and security logs
- **Incident and emergency response**
  - Chain of custody
  - Forensic analysis of compromised system
  - Continuity Of Operation Plan (COOP)
  - Order of volatility

3.0 Research, Analysis and Assessment

3.1 Apply research methods to determine industry trends and impact to the enterprise.

- **Perform ongoing research**
  - Best practices
  - New technologies
  - New security systems and services
  - Technology evolution (e.g., RFCs, ISO)
- **Situational awareness**
  - Latest client-side attacks
  - Knowledge of current vulnerabilities and threats
  - Zero-day mitigating controls and remediation
  - Emergent threats and issues
- **Research security implications of new business tools**
  - Social media/networking
  - End user cloud storage
  - Integration within the business
- **Global IA industry/community**
  - Computer Emergency Response Team (CERT)
  - Conventions/conferences
  - Threat actors
  - Emerging threat sources/ threat intelligence
- **Research security requirements for contracts**
  - Request For Proposal (RFP)
  - Request For Quote (RFQ)
  - Request For Information (RFI)
  - Agreements

3.2 Analyze scenarios to secure the enterprise.

- **Create benchmarks and compare to baselines**
- **Prototype and test multiple solutions**
- **Cost benefit analysis**
  - ROI
  - TCO
- **Metrics collection and analysis**
- **Analyze and interpret trend data to anticipate cyber defense needs**
- **Review effectiveness of existing security controls**
- **Reverse engineer/deconstruct existing solutions**
- **Analyze security solution attributes to ensure they meet business needs**
  - Performance
  - Latency
  - Scalability
  - Capability
  - Usability
  - Maintainability
  - Availability
  - Recoverability
- **Conduct a lessons-learned/ after-action report**
- **Use judgment to solve difficult problems that do not have a best solution**

3.3 Given a scenario, select methods or tools appropriate to conduct an assessment and analyze results.

- **Tool type**
  - Port scanners
  - Vulnerability scanners
  - Protocol analyzer
  - Network enumerator
  - Password cracker
  - Fuzzer
  - HTTP interceptor
  - Exploitation tools/frameworks
  - Passive reconnaissance and intelligence gathering tools
    - Social media
    - Whois
    - Routing tables
- **Methods**
  - Vulnerability assessment
  - Malware sandboxing
  - Memory dumping, runtime debugging
  - Penetration testing
  - Black box
  - White box
  - Grey box
  - Reconnaissance
  - Fingerprinting
  - Code review
  - Social engineering

CompTIA

4.0 Integration of Computing, Communications and Business Disciplines

4.1 Given a scenario, facilitate collaboration 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
- **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**
- **IT governance**

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

- **Security of unified collaboration tools**
  - Web conferencing
  - Video conferencing
  - Instant messaging
  - Desktop sharing
  - Remote assistance
  - Presence
  - Email
  - Telephony
    - VoIP
  - Collaboration sites
    - Social media
    - Cloud-based
- **Remote access**
- **Mobile device management**
  - BYOD
- **Over-the-air technologies concerns**

4.3 Implement security activities across the technology life cycle.

- **End-to-end solution ownership**
  - Operational activities
  - Maintenance
  - Commissioning/decommissioning
  - Asset disposal
  - Asset/object reuse
  - General change management
- **Systems development life cycle**
  - Security System Development Life Cycle (SSDLC)/Security Development Lifecycle (SDL)
  - Security Requirements Traceability Matrix (SRTM)
  - Validation and acceptance testing
  - Security implications of agile, waterfall and spiral software development methodologies
- **Adapt solutions to address emerging threats and security trends**
- **Asset management (inventory control)**
  - Device tracking technologies
    - Geo-location/GPS location
  - Object tracking and containment technologies
    - Geo-tagging/geo-fencing
    - RFID

CompTIA

5.0 Technical Integration of Enterprise Components

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

- **Secure data flows to meet changing business needs**
- **Standards**
  - Open standards
  - Adherence to standards
  - Competing standards
  - Lack of standards
  - De facto standards
- **Interoperability issues**
  - Legacy systems/current systems
  - Application requirements
  - In-house developed vs. commercial vs. commercial customized
- **Technical deployment models (outsourcing/insourcing/ managed services/partnership)**
  - Cloud and virtualization considerations and hosting options
    - Public
    - Private
    - Hybrid
    - Community
    - Multi-tenancy
    - Single tenancy
  - Vulnerabilities associated with a single physical server hosting multiple companies' virtual machines
  - Vulnerabilities associated with a single platform hosting multiple companies' virtual machines
  - Secure use of on-demand/ elastic cloud computing
  - Data remnants
  - Data aggregation
  - Data isolation
  - Resources provisioning and deprovisioning
    - Users
    - Servers
    - Virtual devices
    - Applications
  - Securing virtual environments, services, applications, appliances and equipment
  - 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**
- **Secure infrastructure design (e.g., decide where to place certain devices/applications)**
- **Storage integration (security considerations)**
- **Enterprise application integration enablers**
  - CRM
  - ERP
  - GRC
  - ESB
  - SOA
  - Directory services
  - DNS
  - CMDB
  - CMS

5.2 Given a scenario, integrate advanced authentication and authorization technologies to support enterprise objectives.

- **Authentication**
  - Certificate-based authentication
  - Single sign-on
- **Authorization**
  - OAUTH
  - XACML
  - SPML
- **Attestation**
- **Identity propagation**
- **Federation**
  - SAML
  - OpenID
  - Shibboleth
  - WAYF
- **Advanced trust models**
  - RADIUS configurations
  - LDAP
  - AD

CompTIA

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 a part of a comprehensive exam preparation program.

ACRONYM	SPELLED OUT
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
AIDE	Advanced Intrusion Detection Environment
AJAX	Asynchronous JAVA And XML
ALE	Annualized Loss Expectancy
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threats
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
AUP	Acceptable Use Policy
AV	Antivirus
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
CA	Certificate Authority
CaaS	Communication as a Service
CAC	Common Access Card
CAPTCHA	Completely Automated Public Turning 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

ACRONYM	SPELLED OUT
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
CORS	Cross-Origin Resource Sharing
COTS	Commercial Off-The-Shelf
CRC	Cyclical Redundancy Check
CredSSP	Credential Security Support Provider
CRL	Certification Revocation List
CRM	Customer Resource Management
CSP	Cryptographic Service Provider
CSRF	Cross-Site Request Forgery
CVE	Collaborative Virtual Environment
DAC	Discretionary Access Control
DAM	Database Activity Monitoring
DDoS	Distributed Denial of Service
DEP	Data Execution Prevention
DES	Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic Link Library
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name Service (Server)
DOM	Document Object Model
DoS	Denial of Service
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm
EAP	Extensible Authentication Protocol
ECB	Event Control Block
ECC	Elliptic Curve Cryptography
EFS	Encrypted File System
ELA	Enterprise License Agreement

ACRONYM	SPELLED OUT
EMI	Electromagnetic Interference
EOL	End of Life
ESA	Enterprise Security Architecture
ESB	Enterprise Service Bus
ESP	Encapsulated Security Payload
EV	Extended Validation (Certificate)
FCoE	Fiber Channel over Ethernet
FDE	Full Disk Encryption
FIM	File Integrity Monitoring
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GPG	GNU Privacy Guard
GPU	Graphic Processing Unit
GRC	Governance, Risk and Compliance
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HBA	Host Bus Adapter
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
IDF	Intermediate Distribution Frame
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	Input/Output Controller
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPSec	Internet Protocol Security
IR	Incident Response
IRC	Internet Relay Chat
IS-IS	Intermediate System to Intermediate System
ISA	Interconnection Security Agreement

ACRONYM	SPELLED OUT
ISAC	Information Sharing Analysis Center
iSCSI	Internet Small Computer System Interface
ISMS	Information Security Management System
ISP	Internet Service Provider
IV	Initialization Vector
JSON	JavaScript Object Notation
JWT	JSON Web Token
KDC	Key Distribution Center
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
LOB	Line Of Business
LTE	Long-Term Evolution
LUN	Logical Unit Number
MaaS	Monitoring as a Service
MAC	Mandatory Access Control
MAC	Media Access Control or Message Authentication Code
MAN	Metropolitan Area Network
MBR	Master Boot Record
MD5	Message Digest 5
MDF	Main Distribution Frame
MDM	Mobile Device Management
MEAP	Mobile Enterprise Application Platform
MFD	Multifunction Device
MITM	Man In The Middle
MOA	Memorandum Of Agreement
MOU	Memorandum Of Understanding
MPLS	Multiprotocol Label Switching
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSS	Managed Security Service
MTA	Message Transfer Agent
MTBF	Mean Time Between Failure
MTD	Maximum Tolerable Downtime
MTTR	Mean Time To Recovery
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAS	Network Attached Storage
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
NFS	Network File System
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System

ACRONYM	SPELLED OUT
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 LANMAN
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OFB	Output Feedback
OLA	Operating Level Agreement
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
PACS	Physical Access Control Server
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
PKI	Public Key Infrastructure
PLC	Programmable Logical Controller
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-Shared Key
QA	Quality Assurance
QoS	Quality of Service
R&D	Research and Development
RA	Recovery Agent or Registration Authority
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-In User Server
RAID	Redundant Array of Inexpensive/Independent Disks
RAS	Remote Access Server
RBAC	Role-Based Access Control or Rule-Based Access Control
RDC	Remote Desktop Connection
REST	Representational State Transfer
RFC	Request For Comments
RFI	Request For Information
RFP	Request For Proposal
RFQ	Request For Quote
ROE	Rules of Engagement
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 or 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
SDLM	Software Development Life Cycle Methodology
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
SNAT	Secure Network Address Translation
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture or Start Of Authority
SOAP	Simple Object Access Protocol
SOC	Security Operations Center or Service Organization Controls
SOE	Standard Operating Environment
SOP	Same Origin Policy
SOW	Statement Of Work
SOX	Sarbanes-Oxley Act

ACRONYM	SPELLED OUT
SP	Service Provider
SPIM	Spam Over Internet Messaging
SPIT	Spam over Internet Telephony
SPML	Service Provisioning Markup Language
SRTM	Security Requirements Traceability Matrix
SRTP	Secure Real-Time Protocol
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
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
UDDI	Universal Description Discovery and Integration
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UPN	User Principal Name
UPS	Uninterruptable Power Supply
URL	Universal Resource Locator
USB	Universal Serial Bus

ACRONYM	SPELLED OUT
UTM	Unified Threat Management
VaaS	Voice as a Service
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMFS	Virtual Memory 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 TPM
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
WPA	Wireless Protected Access
WRT	Work Recovery Time
WSDL	Web Services Description Language
WWN	World Wide Name
XACML	eXtensible Access Control Markup Language
XHR	XMLHttpRequest
XMPP	eXtensible Messaging and Presence
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 who wish to create a lab component to their training offering. The bulleted lists below each topic are a sample list and not exhaustive.

EQUIPMENT

- Laptops
- Basic server hardware (email server/ active directory server, trusted OS)
- Basic NAS/SAN
- Tokens
- Mobile devices
- Switches (managed switch) - IPv6 capable
- Router - IPv6 capable
- Gateway
- Firewall
- VoIP
- Proxy server
- Load balancer
- NIPS
- HSM
- Access points
- Crypto-cards
- Smart cards
- Smart card reader
- Biometric devices

SPARE HARDWARE

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

TOOLS

- Spectrum analyzer
- Vulnerability scanner
- Antennas
- Network mapper
- Protocol analyzer

SOFTWARE

- Virtualized appliances (firewall, IPS, SIEM solution, RSA authentication, Asterisk PBX)
- Packets Sniffer
- Windows
- Linux
- VMware player/virtualbox
- Vulnerability assessment tools
- Port scanner
- SSH and Telnet utilities
- Threat modeling tool
- Host IPS
- Helix software
- Kali
- Remediation software
- Open VAS
- Pentest suite
- Metasploit
- GNS
- Honeypot software

OTHER

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

CompTIA