CompTIA Advanced Security Practitioner Certification Exam Objectives

EXAM NUMBER: CAS-002
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 perform a search using CertGuard’s engine, found here.

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 80
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:

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>PERCENTAGE OF EXAMINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Enterprise Security</td>
<td>30%</td>
</tr>
<tr>
<td>2.0 Risk Management and Incident Response</td>
<td>20%</td>
</tr>
<tr>
<td>3.0 Research and Analysis</td>
<td>18%</td>
</tr>
<tr>
<td>4.0 Integration of Computing, Communications and Business Disciplines</td>
<td>16%</td>
</tr>
<tr>
<td>5.0 Technical Integration of Enterprise Components</td>
<td>16%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
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

- **Secure storage management**
  - Multipath
  - Snapshots
  - Deduplication
  - Dynamic disk pools
  - LUN masking/mapping
  - HBA allocation
  - Offsite or multisite replication

- **Encryption**
  - Disk
  - Block
  - File
  - Record
  - Port

CASP Exam Objectives Version 1.0 (Exam Number: CAS-002)
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

- 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)

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
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
  - Deterrence
  - Inherent
  - Residual
- Enterprise security architecture frameworks
- Continuous improvement/monitoring
- Business continuity planning
- IT governance
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)
- 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
- Use general privacy principles for sensitive information (PII)

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
- Method
  - Vulnerability assessment
  - Malware sandboxing
  - Memory dumping, runtime debugging
- Penetration testing
- Black box
- White box
- Grey box
- Reconnaissance
- Fingerprinting
- Code review
- Social engineering

CASP Exam Objectives Version 1.0 (Exam Number: CAS-002)
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

CASP Exam Objectives Version 1.0 (Exam Number: CAS-002)
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

CASP Exam Objectives Version 1.0 (Exam Number: CAS-002)
**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.

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>3DES</td>
<td>Triple Digital Encryption Standard</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorization and Accounting</td>
</tr>
<tr>
<td>AAR</td>
<td>After Action Report</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header</td>
</tr>
<tr>
<td>AJAX</td>
<td>Asynchronous JAVA And XML</td>
</tr>
<tr>
<td>ALE</td>
<td>Annualized Loss Expectancy</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Threats</td>
</tr>
<tr>
<td>ARO</td>
<td>Annualized Rate of Occurrence</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Planning</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input/Output System</td>
</tr>
<tr>
<td>BPA</td>
<td>Business Partnership Agreement</td>
</tr>
<tr>
<td>BPM</td>
<td>Business Process Management</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CaaS</td>
<td>Communication as a Service</td>
</tr>
<tr>
<td>CAC</td>
<td>Common Access Card</td>
</tr>
<tr>
<td>CBC</td>
<td>Cipher Block Chaining</td>
</tr>
<tr>
<td>CCMP</td>
<td>Counter-mode/CBC-Mac Protocol</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-Circuit Television</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>CFB</td>
<td>Cipher Feedback</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CIA</td>
<td>Confidentiality, Integrity and Availability</td>
</tr>
<tr>
<td>CIFS</td>
<td>Common Internet File System</td>
</tr>
<tr>
<td>CIRT</td>
<td>Computer Incident Response Team</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>CMDB</td>
<td>Configuration Management Database</td>
</tr>
<tr>
<td>COOP</td>
<td>Continuity Of Operations</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off-The-Shelf</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclical Redundancy Check</td>
</tr>
<tr>
<td>CredSSP</td>
<td>Credential Security Support Provider</td>
</tr>
<tr>
<td>CRL</td>
<td>Certification Revocation List</td>
</tr>
<tr>
<td>CRM</td>
<td>Customer Resource Management</td>
</tr>
<tr>
<td>CSRF</td>
<td>Cross-Site Request Forgery</td>
</tr>
<tr>
<td>DAC</td>
<td>Discretionary Access Control</td>
</tr>
<tr>
<td>DAM</td>
<td>Database Activity Monitoring</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DEP</td>
<td>Data Execution Prevention</td>
</tr>
<tr>
<td>DES</td>
<td>Digital Encryption Standard</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DLL</td>
<td>Dynamic Link Library</td>
</tr>
<tr>
<td>DLP</td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service (Server)</td>
</tr>
<tr>
<td>DOM</td>
<td>Document Object Model</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>ECB</td>
<td>Event Control Block</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
</tr>
<tr>
<td>EFS</td>
<td>Encrypted File System</td>
</tr>
<tr>
<td>ELA</td>
<td>Enterprise License Agreement</td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
</tr>
<tr>
<td>ESA</td>
<td>Enterprise Security Architecture</td>
</tr>
<tr>
<td>ESB</td>
<td>Enterprise Service Bus</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulated Security Payload</td>
</tr>
<tr>
<td>EV</td>
<td>Extended Validation (Certificate)</td>
</tr>
<tr>
<td>FCoE</td>
<td>Fiber Channel over Ethernet</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GPG</td>
<td>GNU Privacy Guard</td>
</tr>
<tr>
<td>GPU</td>
<td>Graphic Processing Unit</td>
</tr>
<tr>
<td>GRC</td>
<td>Governance, Risk and Compliance</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation</td>
</tr>
<tr>
<td>HBA</td>
<td>Host Bus Adapter</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
</tr>
<tr>
<td>HIDS</td>
<td>Host-based Intrusion Detection System</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>HIPS</td>
<td>Host-based Intrusion Prevention System</td>
</tr>
<tr>
<td>HMAC</td>
<td>Hashed Message Authentication Code</td>
</tr>
<tr>
<td>HOTP</td>
<td>HMAC-based One-Time Password</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>HSTS</td>
<td>HTTP Strict Transport Security</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, Ventilation and Air Conditioning</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control System</td>
</tr>
<tr>
<td>IDF</td>
<td>Intermediate Distribution Frame</td>
</tr>
<tr>
<td>IdM</td>
<td>Identity Management</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange</td>
</tr>
<tr>
<td>IM</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Message Access Protocol</td>
</tr>
<tr>
<td>INE</td>
<td>Inline Network Encryptor</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention Systems</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IRC</td>
<td>Internet Relay Chat</td>
</tr>
<tr>
<td>ISA</td>
<td>Interconnection Security Agreement</td>
</tr>
<tr>
<td>ISMS</td>
<td>Information Security Management System</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>IV</td>
<td>Initialization Vector</td>
</tr>
<tr>
<td>KDC</td>
<td>Key Distribution Center</td>
</tr>
<tr>
<td>KVM</td>
<td>Keyboard, Video, Mouse</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LEAP</td>
<td>Lightweight Extensible Authentication Protocol</td>
</tr>
<tr>
<td>LOB</td>
<td>Line Of Business</td>
</tr>
<tr>
<td>LUN</td>
<td>Logical Unit Number</td>
</tr>
<tr>
<td>MaaS</td>
<td>Monitoring as a Service</td>
</tr>
<tr>
<td>MAC</td>
<td>Mandatory Access Control</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control or</td>
</tr>
<tr>
<td></td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
</tr>
<tr>
<td>MBR</td>
<td>Master Boot Record</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>MDF</td>
<td>Main Distribution Frame</td>
</tr>
<tr>
<td>MDM</td>
<td>Mobile Device Management</td>
</tr>
<tr>
<td>MEAP</td>
<td>Mobile Enterprise Application Platform</td>
</tr>
<tr>
<td>MFD</td>
<td>Multifunction Device</td>
</tr>
<tr>
<td>MITM</td>
<td>Man In The Middle</td>
</tr>
<tr>
<td>MOA</td>
<td>Memorandum Of Agreement</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RA</td>
<td>Recovery Agent or Registration Authority</td>
</tr>
<tr>
<td>RAD</td>
<td>Rapid Application Development</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Server</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Inexpensive/Independent Disks</td>
</tr>
<tr>
<td>RAS</td>
<td>Remote Access Server</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role-Based Access Control or Rule-Based Access Control</td>
</tr>
<tr>
<td>REST</td>
<td>Representational State Transfer</td>
</tr>
<tr>
<td>RFI</td>
<td>Request For Information</td>
</tr>
<tr>
<td>RFP</td>
<td>Request For Proposal</td>
</tr>
<tr>
<td>RFQ</td>
<td>Request For Quote</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir and Adleman</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>RTP</td>
<td>Real-time Transport Protocol</td>
</tr>
<tr>
<td>S/MIME</td>
<td>Secure/Multipurpose Internet Mail Extensions</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertions Markup Language</td>
</tr>
<tr>
<td>SAN</td>
<td>Subject Alternative Name or Storage Area Network</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control And Data Acquisition</td>
</tr>
<tr>
<td>SCAP</td>
<td>Security Content Automation Protocol</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure Copy</td>
</tr>
<tr>
<td>SCSI</td>
<td>Small Computer System Interface</td>
</tr>
<tr>
<td>SDL</td>
<td>Security Development Life Cycle</td>
</tr>
<tr>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>SDLM</td>
<td>Software Development Life Cycle Methodology</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hashing Algorithm</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information Event Management</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SLE</td>
<td>Single Loss Expectancy</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SOA</td>
<td>Service Oriented Architecture or Start Of Authority</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>SOC</td>
<td>Security Operations Center</td>
</tr>
<tr>
<td>SOE</td>
<td>Standard Operating Environment</td>
</tr>
<tr>
<td>SOW</td>
<td>Statement Of Work</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes-Oxley Act</td>
</tr>
<tr>
<td>SP</td>
<td>Service Provider</td>
</tr>
<tr>
<td>SPIM</td>
<td>Spam Over Internet Messaging</td>
</tr>
<tr>
<td>SPIT</td>
<td>Spam over Internet Telephony</td>
</tr>
<tr>
<td>SPML</td>
<td>Service Provisioning Markup Language</td>
</tr>
<tr>
<td>SRTM</td>
<td>Security Requirements Traceability Matrix</td>
</tr>
<tr>
<td>SRTP</td>
<td>Secure Real-Time Protocol</td>
</tr>
<tr>
<td>SSD</td>
<td>Solid State Drive</td>
</tr>
<tr>
<td>SSDLC</td>
<td>Security System Development Life Cycle</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-On</td>
</tr>
<tr>
<td>SSP</td>
<td>Storage Service Provider</td>
</tr>
<tr>
<td>TACACS</td>
<td>Terminal Access Controller Access Control System</td>
</tr>
<tr>
<td>TCO</td>
<td>Total Cost of Ownership</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TOS</td>
<td>Type Of Service</td>
</tr>
<tr>
<td>TOTP</td>
<td>Time-based One-Time Password</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>TSIG</td>
<td>Transaction Signature Interoperability Group</td>
</tr>
<tr>
<td>UAC</td>
<td>User Access Control</td>
</tr>
<tr>
<td>UAT</td>
<td>User Acceptance Testing</td>
</tr>
<tr>
<td>UDID</td>
<td>Universal Description Discovery and Integration</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptable Power Supply</td>
</tr>
<tr>
<td>URL</td>
<td>Universal Resource Locator</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>UTM</td>
<td>Unified Threat Management</td>
</tr>
<tr>
<td>VaaS</td>
<td>Voice as a Service</td>
</tr>
<tr>
<td>VDI</td>
<td>Virtual Desktop Infrastructure</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>vSAN</td>
<td>Virtual Storage Area Network</td>
</tr>
<tr>
<td>VTC</td>
<td>Video Teleconferencing</td>
</tr>
<tr>
<td>VTPM</td>
<td>Virtual TPM</td>
</tr>
<tr>
<td>WAF</td>
<td>Web Application Firewall</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Access Point</td>
</tr>
<tr>
<td>WAYF</td>
<td>Where Are You From</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WIDS</td>
<td>Wireless Intrusion Detection System</td>
</tr>
<tr>
<td>WIPS</td>
<td>Wireless Intrusion Prevention System</td>
</tr>
<tr>
<td>WPA</td>
<td>Wireless Protected Access</td>
</tr>
<tr>
<td>WRT</td>
<td>Work Recovery Time</td>
</tr>
<tr>
<td>WSDDL</td>
<td>Web Services Description Language</td>
</tr>
<tr>
<td>WWN</td>
<td>World Wide Name</td>
</tr>
<tr>
<td>XACML</td>
<td>eXtensible Access Control Markup Language</td>
</tr>
<tr>
<td>XSS</td>
<td>Cross-Site Scripting</td>
</tr>
</tbody>
</table>
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
- Routers - 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

© 2016 CompTIA Properties, LLC, used under license by CompTIA Certifications, LLC. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA Certifications, LLC. CompTIA is a registered trademark of CompTIA Properties, LLC in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA Properties, LLC or of their respective owners. Reproduction or dissemination prohibited without written consent of CompTIA Properties, LLC. Printed in the U.S. 01/16-Feb2016