CompTIA Advanced Security Practitioner (CASP) Certification Exam Objectives

EXAM NUMBER: CAS-003
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:

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>PERCENTAGE OF EXAMINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Risk Management</td>
<td>19%</td>
</tr>
<tr>
<td>2.0 Enterprise Security Architecture</td>
<td>25%</td>
</tr>
<tr>
<td>3.0 Enterprise Security Operations</td>
<td>20%</td>
</tr>
<tr>
<td>4.0 Technical Integration of Enterprise Security</td>
<td>23%</td>
</tr>
<tr>
<td>5.0 Research, Development and Collaboration</td>
<td>13%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
1.0 Risk Management

11 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

12 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)
- 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

CompTIA Advanced Security Practitioner (CASP) Certification Exam Objectives Version 3.0
(Exam Number: CAS-003)
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
- 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 black hole

- **Security zones**
  - DMZ
  - 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)
2.0 Enterprise Security Architecture

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 whitelisting and blacklisting
  - 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**
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

- **Types**
  - Penetration testing
    - Black box
    - White box
    - Gray box
  - Vulnerability assessment
  - Self-assessment
  - Tabletop exercises

- **Host tool types**
  - Password cracker
  - Vulnerability scanner
  - Command line tools
  - Local exploitation tools/frameworks

- **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

- **Physical security tools**
  - Lock picks
  - RFID tools
  - IR camera

- **System 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

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

- Identity propagation

- Federation
  - SAML
  - OpenID
  - Shibboleth
  - WAYF

- Trust models
  - RADIUS configurations
  - LDAP
  - AD

- Attestation

- Identity proofing
Given a scenario, implement cryptographic techniques.

- Techniques
  - Key stretching
  - Hashing
  - Digital signature
  - Message authentication
  - Code signing
  - 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.

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>2FA</td>
<td>Two-Factor Authentication</td>
</tr>
<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 JavaScript 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>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Threat</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>ASLR</td>
<td>Address Space Layout Randomization</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td>AV</td>
<td>Antivirus</td>
</tr>
<tr>
<td>B2B</td>
<td>Business-to-Business</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Planning</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</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>BYOD</td>
<td>Bring Your Own Device</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CAPTCHA</td>
<td>Completely Automated Public Turing test to tell Computers and Humans Apart</td>
</tr>
<tr>
<td>CASB</td>
<td>Cloud Access Security Broker</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>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>CMDB</td>
<td>Configuration Management Database</td>
</tr>
<tr>
<td>CMS</td>
<td>Content Management System</td>
</tr>
<tr>
<td>COOP</td>
<td>Continuity of Operations</td>
</tr>
<tr>
<td>COPE</td>
<td>Corporate Owned, Personally Enabled</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off-the-Shelf</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic 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>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>CSP</td>
<td>Cryptographic Service Provider</td>
</tr>
<tr>
<td>CSRF</td>
<td>Cross-Site Request Forgery</td>
</tr>
<tr>
<td>CTR</td>
<td>Counter Mode</td>
</tr>
<tr>
<td>CVE</td>
<td>Collaborative Virtual Environment</td>
</tr>
<tr>
<td>CYOD</td>
<td>Choose Your Own Device</td>
</tr>
<tr>
<td>DAC</td>
<td>Discretionary Access Control</td>
</tr>
<tr>
<td>DAM</td>
<td>Database Activity Monitoring</td>
</tr>
<tr>
<td>DAR</td>
<td>Data at Rest</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>DKIM</td>
<td>Domain Keys Identified Mail</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</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>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------</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>EDR</td>
<td>Endpoint Detection Response</td>
</tr>
<tr>
<td>EFS</td>
<td>Encrypted File System</td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise Resource Planning</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>FDE</td>
<td>Full Disk Encryption</td>
</tr>
<tr>
<td>FIM</td>
<td>File Integrity Monitoring</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GPG</td>
<td>GNU Privacy Guard</td>
</tr>
<tr>
<td>GPO</td>
<td>Group Policy Object</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>GUI</td>
<td>Graphical User Interface</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>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>laaS</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>IDE</td>
<td>Integrated Development Environment</td>
</tr>
<tr>
<td>IdM</td>
<td>Identity Management</td>
</tr>
<tr>
<td>IdP</td>
<td>Identity Provider</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>IOC</td>
<td>Indicator of Compromise</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPMI</td>
<td>Internet Protocol Multicast Initiative</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention Systems</td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Attached Storage</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NDA</td>
<td>Non-Disclosure Agreement</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>NFS</td>
<td>Network File System</td>
</tr>
<tr>
<td>NGFW</td>
<td>Next Generation Firewall</td>
</tr>
<tr>
<td>NIDS</td>
<td>Network Intrusion Detection System</td>
</tr>
<tr>
<td>NIPS</td>
<td>Network Intrusion Prevention System</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NLA</td>
<td>Network-Level Authentication</td>
</tr>
<tr>
<td>NOS</td>
<td>Network Operating System</td>
</tr>
<tr>
<td>NSP</td>
<td>Network Service Provider</td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
</tr>
<tr>
<td>NTLM</td>
<td>New Technology LAN Manager</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OCSP</td>
<td>Online Certificate Status Protocol</td>
</tr>
<tr>
<td>OLA</td>
<td>Operating-Level Agreement</td>
</tr>
<tr>
<td>OOB</td>
<td>Out-of-Band</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>OTP</td>
<td>One-Time Password</td>
</tr>
<tr>
<td>OVAL</td>
<td>Open Vulnerability Assessment Language</td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer-to-Peer</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol</td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
</tr>
<tr>
<td>PBKDF2</td>
<td>Password-Based Key Derivation Function 2</td>
</tr>
<tr>
<td>PBX</td>
<td>Private Branch Exchange</td>
</tr>
<tr>
<td>PCI-DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>PDP</td>
<td>Policy Distribution Point</td>
</tr>
<tr>
<td>PEAP</td>
<td>Protected Extensible Authentication Protocol</td>
</tr>
<tr>
<td>PEP</td>
<td>Policy Enforcement Point</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
</tr>
<tr>
<td>PII</td>
<td>Personal Identifiable Information</td>
</tr>
<tr>
<td>PIP</td>
<td>Policy Information Point</td>
</tr>
<tr>
<td>PIR</td>
<td>Post Incident Report</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>POC</td>
<td>Proof of Concept</td>
</tr>
<tr>
<td>POTS</td>
<td>Plain Old Telephone Service</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>QA</td>
<td>Quality Assurance</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SNAT</td>
<td>Source Network Address Translation</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SOA</td>
<td>Service-Oriented Architecture</td>
</tr>
<tr>
<td>SOA</td>
<td>Start of Authority</td>
</tr>
<tr>
<td>SOA</td>
<td>Statement of Applicability</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>SOA</td>
<td>Service Organization Controls</td>
</tr>
<tr>
<td>SOE</td>
<td>Standard Operating Environment</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
<tr>
<td>SOW</td>
<td>Statement of Work</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes-Oxley Act of 2002</td>
</tr>
<tr>
<td>SP</td>
<td>Service Provider</td>
</tr>
<tr>
<td>SPIM</td>
<td>Spam over Internet Messaging</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>SRV</td>
<td>Service Records</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>SSD</td>
<td>Service Set Identifier</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>TOC/TOU</td>
<td>Time of Check/Time of Use</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>TTR</td>
<td>Time to Restore</td>
</tr>
<tr>
<td>UAC</td>
<td>User Access Control</td>
</tr>
<tr>
<td>UAT</td>
<td>User Acceptance Testing</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UEFI</td>
<td>Unified Extensible Firmware Interface</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>VDI</td>
<td>Virtual Desktop Infrastructure</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACROYN</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VMFS</td>
<td>VMware File System</td>
</tr>
<tr>
<td>VNC</td>
<td>Virtual Network Connection</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VRRP</td>
<td>Virtual Router Redundancy Protocol</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 Trusted Platform Module</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>WMI</td>
<td>Windows Management Interface</td>
</tr>
<tr>
<td>WPA</td>
<td>Wireless Protected Access</td>
</tr>
<tr>
<td>WRT</td>
<td>Work Recovery Time</td>
</tr>
<tr>
<td>WSDL</td>
<td>Web Services Description Language</td>
</tr>
<tr>
<td>XACML</td>
<td>eXtensible Access Control Markup Language</td>
</tr>
<tr>
<td>XHR</td>
<td>XMLHttpRequest</td>
</tr>
<tr>
<td>XMPP</td>
<td>eXtensible Messaging and Presence Protocol</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 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

**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

**SPARE HARDWARE**
- Keyboards
- Cables
- NICs
- Power supplies
- External USB flash drives

**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

© 2017 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. 08873-Jun2017