CompTIA Advanced Security Practitioner Certification Exam Objectives (CAS-001)

INTRODUCTION

The CompTIA Advanced Security Practitioner (CASP) Certification is a vendor-neutral credential. The CASP exam is an internationally targeted validation of advanced-level security skills and knowledge. While there is no *required* prerequisite, the CASP certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, "hands-on" focus at the enterprise level.

The CASP exam will certify that the successful candidate has the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments. The candidate will apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement solutions that map to enterprise drivers.

The CompTIA Advanced Security Practitioner (CASP) Certification is aimed at an IT security professional who has:

- A minimum of 10 years experience in IT administration including at least 5 years of hands-on technical security experience.

This examination blueprint includes domain weighting, test objectives, and example content. Example topics and concepts are included to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

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

Domain	% of Examination
1.0 Enterprise Security	40%
2.0 Risk Mgmt, Policy/Procedure and Legal	24%
3.0 Research & Analysis	14%
4.0 Integration of Computing, Communications, and Business Disciplines	22%
Total	**100%**

Candidates should have basic knowledge of vendor specific tools and technologies, as this knowledge may be required for the CompTIA 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 who wish to create a lab component to their training offering.

The lists of examples provided in bulleted format below each objective 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.

1.0 Enterprise Security

1.1 Distinguish which cryptographic tools and techniques are appropriate for a given situation.

- Cryptographic applications and proper implementation
- Advanced PKI concepts
    - Wild card
    - OCSP vs. CRL
    - Issuance to entities
    - Users
    - Systems
    - Applications
- Implications of cryptographic methods and design
    - Strength vs. performance vs. feasibility to implement vs. interoperability
- Transport encryption
- Digital signature
- Hashing
- Code signing
- Non-repudiation
- Entropy
- Pseudo random number generation
- Perfect forward secrecy
- Confusion
- Diffusion

1.2 Distinguish and select among different types of virtualized, distributed and shared computing

- Advantages and disadvantages of virtualizing servers and minimizing physical space requirements
- VLAN
- Securing virtual environments, appliances and equipment
- 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
    - Provisioning
    - De-provisioning

    - Data remnants
- Vulnerabilities associated with co-mingling of hosts with different security requirements
    - VMEscape
    - Privilege elevation
- Virtual Desktop Infrastructure (VDI)
- Terminal services

1.3 Explain the security implications of enterprise storage

- Virtual storage
- NAS
- SAN
- vSAN
- iSCSI
- FCOE
- LUN masking
- HBA allocation
- Redundancy (location)
- Secure storage management
    - Multipath
    - Snapshots
    - Deduplication

1.4 Integrate hosts, networks, infrastructures, applications and storage into secure comprehensive solutions

- Advanced network design
    - Remote access
    - Placement of security devices
    - Critical infrastructure / Supervisory Control and Data Acquisition (SCADA)
    - VoIP
    - IPv6
- Complex network security solutions for data flow
- Secure data flows to meet changing business needs
- Secure DNS
    - Securing zone transfer
    - TSIG
- Secure directory services
    - LDAP
    - AD
    - Federated ID
    - Single sign on
- Network design consideration
    - Building layouts
    - Facilities management

- Multitier networking data design considerations
- Logical deployment diagram and corresponding physical deployment diagram of all relevant devices
- Secure infrastructure design (e.g. decide where to place certain devices)
- Storage integration (security considerations)
- Advanced configuration of routers, switches and other network devices
    - Transport security
    - Trunking security
    - Route protection
- ESB
- SOA
- SIEM
- Database Access Monitor (DAM)
- Service enabled
- WS-security

1.5 Distinguish among security controls for hosts

- Host-based firewalls
- Trusted OS (e.g. how and when to use it)
- End point security software
    - Anti-malware
    - Anti-virus
    - Anti-spyware
    - Spam filters
- Host hardening
    - Standard operating environment
    - Security/group policy implementation
    - Command shell restrictions
    - Warning banners
    - Restricted interfaces
- Asset management (inventory control)
- Data exfiltration
- HIPS / HIDS
- NIPS/NIDS

1.6 Explain the importance of application security

- Web application security design considerations
    - Secure: by design, by default, by deployment
- Specific application issues
    - XSS
    - Click-jacking
    - Session management
    - Input validation
    - SQL injection
- Application sandboxing

- Application security frameworks
    - Standard libraries
    - Industry accepted approaches
- Secure coding standards
- Exploits resulting from improper error and exception handling
- Privilege escalation
- Improper storage of sensitive data
- Fuzzing/false injection
- Secure cookie storage and transmission
- Client-side processing vs. server-side processing
    - AJAX
    - State management
    - JavaScript
- Buffer overflow
- Memory leaks
- Integer overflows
- Race conditions
    - Time of check
    - Time of use
- Resource exhaustion

1.7 Given a scenario, distinguish and select the method or tool that is appropriate to conduct an assessment

- Tool type
    - Port scanners
    - Vulnerability scanners
    - Protocol analyzer
    - Switchport analyzer
    - Network enumerator
    - Password cracker
    - Fuzzer
    - HTTP interceptor
    - Attacking tools/frameworks
- Methods
    - Vulnerability assessment
    - Penetration testing
    - Black box
    - White box
    - Grey Box
    - Fingerprinting
    - Code review
    - Social engineering

2.0 Risk Management, Policy / Procedure and Legal

2.1 Analyze the security risk implications associated with business decisions

- Risk management of new products, new technologies and user behaviors
- New or changing business models/strategies
    - Partnerships
    - Outsourcing
    - Mergers
- Internal and external influences
    - Audit findings
    - Compliance
    - Client requirements
    - Top level management
- Impact of de-perimiterization (e.g. constantly changing network boundary)
    - Considerations of enterprise standard operating environment (SOE) vs. allowing personally managed devices onto corporate networks

2.2 Execute and implement risk mitigation strategies and controls

- Classify information types into levels of CIA based on organization/industry
- Determine aggregate score of CIA
- Determine minimum required security controls based on aggregate score
- Conduct system specific risk analysis
- Make risk determination
    - Magnitude of impact
    - Likelihood of threat
- Decide which security controls should be applied based on minimum requirements
    - Avoid
    - Transfer
    - Mitigate
    - Accept
- Implement controls
- ESA frameworks
- Continuous monitoring

2.3 Explain the importance of preparing for and supporting the incident response and recovery process

- E-Discovery
    - Electronic inventory and asset control
    - Data retention policies
    - Data recovery and storage
    - Data ownership
    - Data handling
- Data breach
    - Recovery
    - Minimization
    - Mitigation and response

- System design to facilitate incident response taking into account types of violations
    - Internal and external
    - Privacy policy violations
    - Criminal actions
    - Establish and review system event and security logs
- Incident and emergency response

2.4 Implement security and privacy policies and procedures based on organizational requirements.

- Policy development and updates in light of new business, technology and environment changes
- Process/procedure development and updated 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
    - 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 PII / Sensitive PII
- Support the development of policies that contain
    - Separation of duties
    - Job rotation
    - Mandatory vacation
    - Least privilege
    - Incident response
    - Forensic tasks
    - On-going security
    - Training and awareness for users
    - Auditing requirements and frequency

3.0 Research and Analysis

3.1 Analyze industry trends and outline potential impact to the enterprise

- Perform on-going research
    - Best practices
    - New technologies
    - New security systems and services
    - Technology evolution (e.g. RFCs, ISO)
- Situational awareness
    - Latest client-side attacks

    - Threats
    - Counter zero day
    - Emergent issues
- Research security implications of new business tools
    - Social media/networking
    - Integration within the business (e.g. advising on the placement of company material for the general public)
- Global IA industry/community
    - Conventions
    - Attackers
    - Emerging threat sources
- Research security requirements for contracts
    - Request for Proposal (RFP)
    - Request for Quote (RFQ)
    - Request for Information (RFI)
    - Agreements

3.2 Carry out relevant analysis for the purpose of securing the enterprise

- Benchmark
- Prototype and test multiple solutions
- Cost benefit analysis (ROI, TCO)
- Analyze and interpret trend data to anticipate cyber defense aids
- Review effectiveness of existing security
- Reverse engineer / deconstruct existing solutions
- Analyze security solutions to ensure they meet business needs
    - Specify the performance
    - Latency
    - Scalability
    - Capability
    - Usability
    - Maintainability
    - Availability (MTTR, MTBF)
- Conduct a lessons-learned / after-action review
- Use judgment to solve difficult problems that do not have a best solution
- Conduct network traffic analysis

4.0 Integration of Computing, Communications and Business Disciplines

4.1 Integrate enterprise disciplines to achieve secure solutions

- Interpreting security requirements and goals to communicate with other disciplines
    - Programmers
    - Network engineers
    - Sales staff

- Provide guidance and recommendations to staff and senior management on security processes and controls
- Establish effective collaboration within teams to implement secure solutions
- Disciplines
    - Programmer
    - Database administrator
    - Network administrator
    - Management
    - Stake holders
    - Financial
    - HR
    - Emergency response team
    - Facilities manager
    - Physical security manager

4.2 Explain the security impact of inter-organizational change

- Security concerns of interconnecting multiple industries
    - Rules, policies and regulations
- Design considerations during mergers, acquisitions and de-mergers
- Assuring third party products - only introduce acceptable risk
    - Custom developed
    - COTS
- Network secure segmentation and delegation
- Integration of products and services

4.3 Select and distinguish the appropriate security controls with regard to communications and collaboration

- Unified communication security
    - Web conferencing
    - Video conferencing
    - Instant messaging
    - Desktop sharing
    - Remote assistance
    - Presence
    - Email
    - Telephony
- VoIP security
- VoIP implementation
- Remote access
- Enterprise configuration management of mobile devices
- Secure external communications
- Secure implementation of collaboration platforms
- Prioritizing traffic (QoS)
- Mobile devices
    - Smart phones, IP cameras, laptops, IP based devices

4.4 Explain advanced authentication tools, techniques and concepts

- Federated identity management (SAML)
- XACML
- SOAP
- Single sign on
- SPML
- Certificate based authentication
- Attestation

4.5 Carry out security activities across the technology life cycle

- End to end solution ownership
- Understanding results of solutions in advance
    - Operational activities
    - Maintenance
    - Decommissioning
    - General change management
- Systems Development Life Cycle
    - Security System Development Life Cycle (SSDLC) / Security Development Life Cycle (SDL)
    - Security Requirements Traceability Matrix (SRTM)
- Adapt solutions to address emerging threats and security trends
- Validate system designs

CASP ACRONYMS

3DES – Triple Digital Encryption Standard
AAA – Authentication, Authorization, and Accounting
ACL – Access Control List
AD—Active Directory
AES - Advanced Encryption Standard
AES256 – Advanced Encryption Standards 256bit
AH - Authentication Header
ALE - Annualized Loss Expectancy
AP - Access Point
ARO - Annualized Rate of Occurrence
ARP - Address Resolution Protocol
AUP - Acceptable Use Policy
BCP – Business Continuity Planning
BIOS – Basic Input / Output System
BOTS – Network Robots
BPA - Business Partnership Agreement
CA – Certificate Authority
CAC - Common Access Card
CAN - Controller Area Network
CCMP – Counter-Mode/CBC-Mac Protocol
CCTV - Closed-circuit television
CERT – Computer Emergency Response Team
CHAP – Challenge Handshake Authentication Protocol
CIA - Cryptographic Information Application
CIA – Confidentiality, Integrity, and Availability
CIFS- Common Internet File System
CIRT – Computer Incident Response Team
CISO – Chief Information Security Officer
CMDB- Configuration Management Database
COOP- Continuity of Operations
CRC – Cyclical Redundancy Check
CredSSP – Credential Security Support Provider
CRL – Certification Revocation List
CRM- Customer Relationship Management
DAC – Discretionary Access Control
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)
DOS – Denial of Service

DRP – Disaster Recovery Plan
DSA – Digital Signature Algorithm
EAP - Extensible Authentication Protocol
ECC - Elliptic Curve Cryptography
EFS – Encrypted File System
ELA- Enterprise License Agreement
EMI – Electromagnetic Interference
ESA- Enterprise Security Architecture
ESB—Enterprise Service Bus
ESP – Encapsulated Security Payload
FCOE – Fiber Channel Over Ethernet
FTP – File Transfer Protocol
GPU - Graphic Processing Unit
GRC – Governance, Risk, & Compliance
GRE - Generic Routing Encapsulation
HBA- Host Based Adapter
HBA – Host Based Authentication
HDD – Hard Disk Drive
HIDS – Host Based Intrusion Detection System
HIPS – Host Based Intrusion Prevention System
HMAC – Hashed Message Authentication Code
HSM – Hardware Security Module
HTTP – Hypertext Transfer Protocol
HTTPS – Hypertext Transfer Protocol over SSL
HVAC – Heating, Ventilation Air Conditioning
IaaS - Infrastructure as a Service
ICMP - Internet Control Message Protocol
ID – Identification
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
IMAP4 - Internet Message Access Protocol v4
IP - Internet Protocol
IPS – Intrusion Prevention Systems
IPSec – Internet Protocol Security
IRC - Internet Relay Chat
ISA--Interconnection Security Agreement
ISP – Internet Service Provider
IV - Initialization Vector
KDC - Key Distribution Center
L2TP – Layer 2 Tunneling Protocol
LANMAN – Local Area Network Manager

LDAP – Lightweight Directory Access Protocol
LEAP – Lightweight Extensible Authentication Protocol
LUN – Link Uninhibit
MAC – Mandatory Access Control / Media Access Control
MAC - Message Authentication Code
MAN - Metropolitan Area Network
MBR – Master Boot Record
MD5 – Message Digest 5
MDF- Main Distribution Frame
MFD- Multifunction Device
MOA- Memorandum of Agreement
MOU--Memorandum of Understanding
MPLS – Multiprotocol Label Switching
MSCHAP – Microsoft Challenge Handshake Authentication Protocol
MSS – Managed Security Service
MTBF- Mean-Time Between Failure
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
NIDS – Network Based Intrusion Detection System
NIPS – Network Based Intrusion Prevention System
NIST – National Institute of Standards & Technology
NLA – Network Level Authentication
NOS – Network Operating System
NTFS - New Technology File System
NTLM – New Technology LANMAN
NTP - Network Time Protocol
OCSP—Online Certificate Status Protocol
OLA--Operating Level Agreement
ORB- Object Request Broker
OS – Operating System
OVAL – Open Vulnerability Assessment Language
PaaS- Platform as a Service
PAP – Password Authentication Protocol
PAT - Port Address Translation
PBX – Private Branch Exchange
PCI-DSS- Payment Card Industry Data Security Standard
PDP- Policy Distribution Point
PEAP – Protected Extensible Authentication Protocol
PED - Personal Electronic Device
PEP- Policy Enforcement Point
PFS- Perfect Forward Secrecy
PGP – Pretty Good Privacy

PII – Personally Identifiable Information
PII-Personal Identifiable Information
PIP- Policy Information Point
PKI – Public Key Infrastructure
POTS – Plain Old Telephone Service
PPP - Point-to-point Protocol
PPTP – Point to Point Tunneling Protocol
PSK – Pre-Shared Key
PTZ – Pan-Tilt-Zoom
QoS- Quality of Service
RA – Recovery Agent
RAD - Rapid application development
RADIUS – Remote Authentication Dial-in User Server
RAID – Redundant Array of Inexpensive Disks
RAS – Remote Access Server
RBAC – Role Based Access Control
RBAC – Rule Based Access Control
RFI- Request for Information
RFP- Request for Proposal
RFQ- Request for Quote
RSA – Rivest, Shamir, & 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 – Storage Area Network
SCADA—Supervisory Control and Data Acquisition
SCAP - Security Content Automation 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
SHA – Secure Hashing Algorithm
SHTTP – Secure Hypertext Transfer Protocol
SIEM- Security Information Event Management
SIM – Subscriber Identity Module
SLA – Service Level Agreement
SLA--Service Level Agreement
SLE - Single Loss Expectancy
S/MIME – Secure / Multipurpose Internet Mail Extensions
SMS - Short Message Service
SMTP – Simple Mail Transfer Protocol
SNMP - Simple Network Management Protocol
SOAP--Simple Object Access Protocol

SOA- Service Oriented Architecture
SOA--Start of Authority
SOE- Standard Operating Environment
SONET – Synchronous Optical Network Technologies
SOX- Sarbanes–Oxley Act
SP- Service Provider
SPIM - Spam over Internet Messaging
SPIT- Spam over Internet Telephony
SPML- Service Provisioning Markup Language
SRTM- Software Requirements Traceability Matrix
SRTP – Secure Real-time Protocol
SSD- Solid State Drive
SSDLC-- Security System Development Life Cycle
SSH – Secure Shell
SSL – Secure Sockets Layer
SSO – Single Sign On
STP – Shielded Twisted Pair
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
TPM – Trusted Platform Module
TSIG- Transaction Signature Interoperability Group
UAC – User Access Control
UAT - User Acceptance Testing
UDDI- Universal Description Discovery and Integration
UDP – User Datagram Protocol
UPS - Uninterruptable Power Supply
URL - Universal Resource Locator
USB – Universal Serial Bus
UTP – Unshielded Twisted Pair
VDI—Virtual Desktop Infrastructure
VLAN – Virtual Local Area Network
VoIP - Voice over IP
VPN – Virtual Private Network
vSAN – Virtual Storage Area Network
VTC – Video Teleconferencing
WAC- Web Access Control
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
WSDL- Web Services Description Language
XSRF - Cross-Site Request Forgery
CSRF- Cross-Site Request Forgery
XACML- eXtensible Access Control Markup Language
XSS - Cross-Site Scripting

CASP Proposed Hardware and Software List

**Candidates should have basic knowledge of vendor specific tools and technologies, as this knowledge may be required for the CompTIA CASP Certification Exam. 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.

Equipment

- Laptops
- Virtualized appliances (firewall, IPS, SIEM solution, RSA authentication, Asterisk PBX)
- Basic server hardware (Email server/active directory server, trusted OS)
- Basic NAS ("Free NAS")
- Tokens
- Mobile devices
- 2 switches (managed switch) – IPv6 capable
- Router - IPv6 capable
- Gateway
- WAP
- WAF
- IPv6 and IPv4
- Proxy server
- Load balancer
- CA server

Spare hardware

- NICs
- Power supplies
- External USB flash drive
- Access points

Spare parts

- Patch cables

Software

- Packet Sniffer
- Vulnerable web applications (web-goat, hacme bank, dvl)
- Windows
- Linux
- VMWare player / Virtualbox
- Vulnerability assessment tools
- Visio (diagramming software)
- Port scanner
- SSH and Telnet utilities
- Threat modeling tool
- Host IPS
- Helix software
- Backtrack CD

Other

- Sample logs
- Sample network traffic (pcap)
- Sample organizational structure
- Sample network documentation