CompTIA's Advanced Security Practitioner (CASP) Certification Study Guide and Practical Questions

Table of Contents

Exam Overview

Problem Statement: The cyberspace and its infrastructure are unprotected to several risks which stem from both a physical and cyber threats. By exploiting these vulnerabilities, the cybercriminals acquire sensitive information and prevent the delivery of crucial IT services to the users.

The CompTIA's Advanced Security Practitioner (CASP), CAS-002, certification is a vendor-neutral and expert-level credential that provides the best information security solutions for both government agencies and Non-Governmental Organizations (NGOs).

Furthermore, the CASP certification meets the ISO17024 standards and is approved by the US Department of Defense (USDOD). Also, the CASP credential has gained stupendous popularity in the IT security arena due to its worldwide recognition. The director of services at Aspen Skiing Co, Robert Blanchard, says "the person with CASP credential quickly gets hired."

Think You're Ready To Tackle The CASP Exam? Take This Free Assessment & Find Out

Test Details

The following Table contains all the details about CASP test.

Exam Code:	CAS-002
Language:	English
Number of Questions:	Maximum of ninety (90)
Types of Questions:	Performance-based and multiple choice
Length of Test:	One hundred and sixty-five (165) minutes
Recommended Experience:	Ten (10) years of experience in IT administration, including at least five (5) years of hands-on technical security experience.
Passing Score:	No scaled score just Pass/Fail only.
Validity:	Three (3) years after launch
Price:	$426

What are the Exam Domains (Objectives)?

The underlying Table contains the exam domains and their percentage.

Domains	Percentage Of The Examination
1—Enterprise Security	30%
2—Risk Management and Incident Response	20%
3—Research and Analysis	18%
4—Integration of Computing, Communication, and Business Disciplines	16%
5—Technical Integration of Enterprise Components	16%
Total	100%

Test Day Rules

The candidate must bring his/her two identification forms in the testing center. Besides, the electronic devices are prohibited during the test. These devices include:

- Smartphone
- Smart watches
- Notebook computer
- Tablet

CASP Pricing

The following Table includes the list of different countries and the prices they offer for CASP certification.

Country	Currency	Price
Thailand	THB	13,320
New Zealand	NZD	456
Japan	JPY	45,270
EURO	EURO	387
Malaysia	MYR	1,518
South Africa	ZAR	2,770
Australia	AUD	425
Malaysia	MYR	1518
England	GBP	267
Emerging Market	USDe	400
Switzerland	CHF	548
USA	USD	426

Recommended Experienced

The CASP candidate is required to have ten (10) years of experience in IT administration, including at least five (5) years of hands-on technical security experience.

How to Schedule the Exam?

Once the candidate meets all the CASP's requirements, he/she could schedule the exam on CompTIA's website by following some steps, including:

1. Buy exam voucher
2. Create login account
3. Find a testing center
4. Save exam details

CASP Renewal Cycle

CompTIA provides a Continuing Education (CE) program that assists the aspirants to keep their credentials up-to-date to attain longevity and advancement in their job tenure. As an IT is a rapidly changing field, the new opportunities and challenges are being created every day. The CE program helps the candidates to stay current with modern technologies and emerging trends in IT market.

The CASP credential is valid for three years, and the candidates are advised to extend his/her certification in 3-year time using CE policy. For this purpose, the participation in various activities and training programs is also essential for the candidates.

Automatic Renewal: it allows the students to automatically renew their credentials by collection a minimum of seventy-five (75) Continuing Education Units (CEUs) in three (3) years. The candidates should upload the CEUs in the certification account to automatically renew their credential.

Renewal charges: these charges are mandatory for the students. The due dates of the fee are based on CE renewal process, not on calendar years. When the expiry date comes along, the aspirant is informed through periodic Emails that remind him/her to upload CEU documentations. The annual CE charges are 50 USD and 150 USD for three-years (3).

With Easy Payment, the candidates have the choice to pay their dues with different payment methods, including:

- Use the current PayPal account
- Use the Debit or the Credit card (VISA, Master Card, American Express, Discover)

Also, the students are not required to have a PayPal account to pay with a debit or credit cards.

If the candidates have **multiple CompTIA certifications**, he/she doesn't need to pay for each to renew them separately. Rather, she/he will only pay CE fees for the highest-level CompTIA certification; the lower-level credentials will automatically be renewed without paying any additional charges.

CompTIA also gives **CE Tokens** to their members to facilitate them in paying their CE dues.

Why Should You Get the CASP Credential?

CASP is a popular certification in the IT industry worldwide and it has numerous benefits, including:

Skills Development

IT security professionals having CASP certification will be able:

- To apply judgment and critical thinking across a vast spectrum of security disciplines to provide and implement viable security solutions that map out the organizational strategies.
- To conceptualize, integrate, engineer and then apply the sustainable solutions across complex environments.

- To translate business needs into the security requirements.
- Respond to security incidents.
- To analyze the risk impact.

Global Recognition

CompTIA is the vendor who provides CASP certification. CompTIA has recognized worldwide as the leading IT nonprofit trade association and its credibility is undoubted. Therefore, getting CASP is highly valuable especially for those seeking for immediate employment.

CASP Accreditation

CASP certification is accredited by the ANSI (American National Standards and Institute) to indicate compliance with the ISO-17024 standard.

Recommended by Government and Business

Various governmental and Non-governmental organization (NGOs) organizations recommend CompTIA's CASP certification. These organizations include U.S Department of Defense (UDD), Ricoh, Sharp, and Dell, and various others.

What are the CASP Core Concepts?

To become a CASP-certified, the candidates must understand the core concepts in CASP domains. As aforementioned, the candidate should know about the enterprise security, Risk Management and incident response, integration of business disciplines, and technical integration of core concepts.

1. Enterprise Risk

CASP plays a crucial role in enterprise security and risk management by providing recommendations and guidance to executives and employees on the security controls and processes. These recommendations include the understanding of cryptographic solutions, PKI, digital signature and hashing, advanced network design, security controls for hosts, and application vulnerability and security controls.

Cryptographic Solutions

The most efficient cryptographic solutions include symmetric cryptography, asymmetric cryptography, hashing, and hybrid encryption. Each solution ensures confidentiality, integrity, and authentication of data in the organizations.

Understand Public Key Infrastructure (PKI)

PKI solution is used to protect the public key used in symmetric cryptography. In a symmetric encryption scheme, both the sender and the receiver used the same key to encrypt and decrypt the text or message.

Digital Signatures and Hashing

Digital signatures prove that a message was sent from a specific user and that the message wasn't altered while in transit. Hashing is used to protect the integrity of a message by preventing it from being illegitimately accessed during transmits over the network.

Advanced Network Design

The CASP professionals should understand some important concepts in advanced network design including remote access, network authentication methods, transport encryption, 802.1x, mesh networks, and IPv4 and associated transitional technologies.

Security Controls for Hosts

The security professional must understand that the operating system (OS) must be protected or trusted. Also, how trusted OS can be used to improve the security of the system. Furthermore, the security experts also understand some security software, such as antispyware, antivirus, antimalware, spam filter, HIPS/HIDS, firewalls, log monitoring, and patch management.

Applications Vulnerabilities and Security Controls

The CASP professionals need to know the principles of secure web application design. The guidelines are developed by common application vulnerability category including authentication, input validation, authorization, cryptography, parameter manipulation, session management, sensitive data, and configuration management. The candidates also understand some issues associated with the application, such as Cross-Site Request Forgery (CSRF), direct object references, SQL injection, fault injection, insecure cookies storage, privilege escalation, improper storage of sensitive data, and incorrect error and exception handling.

2. Risk Management and Incident Response

The CASP professionals must understand the threats to the organizations, potential risks, and the ways to mitigate risks.

Business Models

In the age of globalization, the markets have evolved from one country to another country and even from one continent to another continent. The business community has interlinked with one another. From the IT perspective, such partnerships or business connections may encounter various security risks. To thwart such risks, the CASP-certified must be aware of the **business models** that include:

- Partnerships
- Outsourcing
- Mergers
- Acquisitions

Internal and External Influences

There are various factors involved to control the markets. In industrialized states, such as the United States and China, the companies have developed their own policies or code of conduct that define the operational activities of these enterprises that also involve their management and employees. The internal factors include the high-level policies and audit findings can have a great impact on business operations.

Understand the Change in Network Boundaries

The Could Computing, in fact, obscures the network boundaries as the exact site of particular data may be unknown. The protection mechanisms provided by the cloud providers are also difficult to understand. Contrarily, by 1990, the networks were easy to define with defensive technologies that include firewalls and Intrusion Detection Systems (IDSs).

Risks of Manageable Devices in Corporate Environment

Today, almost everyone is familiar with mobile devices, iPads, PDAs, and smart watches. These devices can be used to intrude in corporate IT environment and they are great concerns for the IT security professionals. To deal with such risks, the corporate has developed its policies that define what is allowed and what is disallowed in corporation network.

Understand Confidentiality, Integrity, and Availability (CIA)

CIA is the modern security principles that are applied to the risk assessment process in companies. The CASP candidate must understand these concepts. Confidentiality is the act of ensuring that the information is unavailable to unauthorized individuals. Integrity assures that the information isn't altered during the transit over a network. In a nutshell, the job of security professional is to protect the confidentiality, availability, and integrity of companies' valuable informational assets.

Risk Analysis Techniques

There are two fundamental techniques to carry out risk analysis: Quantitative and Qualitative. The Quantitative risk assessment is a dollar-based and assigns dollar amounts to known risks. On the other hand, the Qualitative risk assessment is a non-dollar-based and employs attributes, such as critical, low, medium, and high.

Know How to Make a Risk Determination Analysis

Risks and vulnerability assessment is crucial for company's IT infrastructure and the security of its assets. The IT professionals (assessors) can provide recommendations for increasing the level of security of corporations' assets.

Various Ways to Address Risks

The CASP candidates must learn the approaches used to prevent the threats and vulnerabilities. Different methods can be used to prevent the potential hazards. The methods include avoid, accept, transfer, or mitigate.

Components of an Incident Response Plan

The CASP candidate must develop a plan to better respond to any incident. The following number of steps should be performed when an incident occurs:

1. Planning and preparation
2. Identification and Evaluation
3. Containment and Mitigation
4. Eradication and Recovery
5. Investigation and closure

Basic Forensic Tasks

Basie Forensic tasks include:

1. Identification
2. Presentation
3. Collection
4. Examination
5. Analysis
6. Presentation of Findings

3. Research and Analysis

The research and analysis domain of CASP exam focus on two broad areas:

- Analyze industry trends and summarizing potential impact to the enterprises
- Determine relevant analysis aims at securing the enterprises

Performing Ongoing Research

Performing ongoing research means the CASP professional must reviews industry trends and summarizes the potential impact to enterprises. To do so, he/she is required to understand modern technologies, to know how to evaluate current systems, and to understand standards and documentation, such as ISOs, NIST, and RFCs.

Situational Awareness

Situational awareness required the CASP professionals to always aware of security incidents, such as threats and client-side attacks, which may be happened in organizations and how to deal with such incidents.

Global IA Industry

CASP professionals must need to know how to interface with other businesses in the global IA industry. The best way is to participate in security events and conferences that held each year, such as DefCon (world's largest hacker convention).

Relevant Analysis

The security professionals carry out the relevant analysis to secure the enterprises. To perform relevant analysis, the CASP professional must understand RFIs, RFQs, and RFPs. He/she also ensures that the agreements meet the security requirements of the company.

Network Traffic Analysis

The network analysis is performed by placing a sniffer, such as "Wireshark" on segments of a network and acquiring network traffic.

4. Enterprise Security Integration

The CASP professionals need to know how to deploy security solutions in the organizations.

Need to Integrate Business Disciplines to attain Secure Solutions

The CASP professionals work with others in the organizations to integrate the needs of the companies into the comprehensive security solutions. The holistic security solution is necessary for enterprise's continuity of business operations. Also, these solutions help in maintaining the confidentiality and integrity of companies' data.

Role of Governance in Attaining Organization Security

Governance is all about management, control of the enterprise, customs, processes, and policies or code of ethics. The top management in the company is responsible for ensuring the development, implementation, and compliance of rules and regulations so that the IT infrastructure could be controlled.

Employee Controls

Employee control mechanisms provide the understanding how new employees are hired and how their expulsion and retirements are managed. The examples of good employee control include the least privilege, dual controls, and mandatory vacations.

Learn the Control Types

There are three control types, such as administrative controls, technical controls, and physical controls. The CASP professional use one of these controls to provide recommendations and guidance to employees and top management.

Understand the Various Disciplines

There should be an explicit division of disciplines, roles, and responsibilities within the enterprise. The discipline includes the consultants, vendors, and employees. All of them must comply with company's security policy.

Understand the Impact of Inter-organizational Change

The inter-organizational change often reduces the security level of system configurations within the enterprises. The CASP professionals use *Change Control Processes* to avoid the unwanted consequences occurring due to the organizational change.

Security Issues when Interconnecting Multiple Industries

When two or more enterprises or their networks are interconnected, there is a huge risk of a security breach which allows the cybercriminals to migrate from one company to another through viruses or phishing techniques.

Deployment Techniques

Deployment techniques are used to integrate products and services into the environment. Three deployment techniques include the Hard Changeover, Phased, and Parallel.

5. Technical Integration of Enterprise Components

Host, Network, Storage, and Application Integration into the Secure Enterprise Architecture

The data flow must be secured to meet rapidly changing business needs. To do so, the security professionals deploy security controls when business needs are changed. Also, understanding of standards is essential in CASP exam that includes open standards, competing standards, de facto standards, lack of standards, and adherence to standards. Some other important concepts for exam point of view include technical deployment models, secure infrastructure design, storage integration, and enterprise application integration enablers.

Authentication and authorization technologies

For CASP exam, authentication includes single sign-on and certificate-based authentication. Also, the candidate would learn the methods of authorization, such as SPML, XACML, and OAUTH. Besides, the candidates also learn the Attestation and its purposes as it relates to trusted and secure computing. Other important concepts include identity propagation, federation, and advanced trusted models.

SAML, OpenID, and Shibboleth

Security Assertion Markup Language (SAML) is an open standard that provides both authorization and authentication. The current version of SAML is SAML2.0.

OpenID is the open standard just for authentication. It's promoted by the nonprofit organization known as OpenID Foundation. Currently, billions of users are using OpenID-enabled accounts on the internet. Also, many organizations use OpenID to authenticate their users. These organizations include PayPal, WordPress, Yahoo, and Google.

Shibboleth is a single log-in system for computer networks, and it allows users to sign-in using just one identity to several systems run by the Federation of different institutions or organizations.

Proposed Hardware and Software List for CASP

CompTIA included the hardware and software list to help the candidates for exam preparation. Also, this list is helpful to those training companies who want to establish lab components to their training offering.

TOOLS
Protocol Analyzer
Antennas
Network mapper
Vulnerability scanner
Spectrum analyzer

EQUIPMENT

Biometric devices
Crypto-cards
Access points
NIPS
Load Balancer
VoIP
Router and Switches
Tokens
Mobile devices and Laptops
Basic SAN/NAS

SPARE HARDWARE
External USB Flash Drives
Power Supplies
NICs
Cables

Keyboards

SOFTWARE
Honeypot software
GNS
Open VAS
Helix software
Host IPS
Threat modeling tool
Port scanner
Vulnerability assessment tool
VMware player/virtual box
Linux
Windows
Packets Sniffer
Virtualized appliances (IPS, Firewall)

OTHER
3G/4G hotspot
Broadband Internet connection
Sample organizational structure
Sample Network traffic
Sample logs
Sample network documentation

CASP Acronyms

The underlying Table contains a list of acronyms that are necessary for CASP exam. For a comprehensive exam preparation, the candidates must know all listed acronyms.

ACRONYM	SPELLED OUT	ACRONYM	SPELLED OUT
AAA	Authentication, Authorization, and Accounting	ELA	Enterprise License Agreement
AAR	After Action Report	ECC	Elliptic Curve Cryptography
AD	Active Directory	ECB	Event Control Block
AUP	Acceptable Use Policy	ESB	Enterprise Service Bus
ARO	Annualized Rate of Occurrence	FDE	Full Disk Encryption
API	Application Programming Interface	FIPS	Federal Information Processing Standard
AJAX	Asynchronous Java And XML	GUI	Graphical User Interface
AV	Antivirus	GRC	Governance, Risk and Compliance
BPM	Business Process Management	GPG	GNU Privacy Guard
BIOS	Basic Input/Output System	HVAC	Heating, Ventilation and Air Conditioning
BGP	Border Gateway Protocol	HSM	Hardware Security Module
BCP	Business Continuity Planning	HIPS	Host-based Intrusion Prevention System
CA	Certificate Authority	HIDS	Host-based Intrusion Detection System

CASB	Cloud Access Security Broker	HDD	Hard Disk Drive
CaaS	Communication as a Service	HBA	Host Bus Adapter
CIA	Confidentiality, Integrity, and Availability	HIMAC	Hashed Message Authentication Code
CRM	Customer Resource Management	IPSec	Inter Protocol Security
CRC	Cyclical Redundancy Check	IPS	Intrusion Prevention System
CMS	Content Management System	IP	Internet Protocol
CLI	Command Line Interface	IOC	Input /Output Controller
CISO	Chief Information Security Officer	IMAP	Internet Message Access Protocol
DR	Disaster Recovery	IDS	Intrusion Detection System
DoS	Denial of Service	IR	Incident Response
DNS	Domain Name Server (Service)	ISMS	Information Security Management System
ISP	Internet Service Provider	PSK	Pre-shared Key
LTE	Long-Term Evolution	PPP	Point-to-Point Protocol
LEAP	Lightweight Extensible Authentication Protocol	PEAP	Protected Extensible Authentication Protocol
LDAP	Lightweight Directory Access Protocol	PCI-DSS	Payment Card Industry Data Security Standard
L2TP	Layer 2 Tunneling Protocol	PAP	Password Authentication Protocol
LAN	Local Area Network	QoS	Quality of Service
MaaS	Monitoring as a Service	RBAC	Rule-Based Access Control or Role-Based Access Control
MPLS	Multiprotocol Label Switching	RAD	Rapid Application Development
MOU	Memorandum of Understanding	R&D	Research and Development
MOA	Memorandum of Agreement	RDC	Remote Desktop Connection
MFD	Multifunction Device	RTP	Real-time Transport Protocol
MD5	Message Digest 5	ROI	Return On Investment
MAN	Metropolitan Area Network	REST	Representational State Transfer
NTP	New Technology LANMAN	SSP	Storage Service Provider
NTFS	New Technology File System	SSL	Secure Sockets Layer
NSP	Network Service Provider	SSD	Solid State Drive
NOS	Network Operating System	SP	Service Provider
NIPS	Network-based Intrusion Prevention System	SPML	Service Provisioning Markup Language
NIDS	Network-based Intrusion Detection System	SOA	Service Oriented Architecture or Start Of Authority
NDA	Non-Disclosure Agreement	SOAP	Service Organization Controls or Simple Object Access Protocol
		SOC	Security Operations Center
NAC	Network Access Control	SOW	Statement Of Work
OSI	Open Systems Interconnection	SOP	Same Origin Policy
OS	Operating System	SOX	Same Origin Policy
OCSP	Online Certificate Status	SDLM	Software Development Life Cycle

	Protocol		Methodology
OTP	One-Time Password	SDLC	Software Development Life Cycle
PaaS	Platform as a Service	SDL	Security Development Life Cycle
PGP	Pretty Good Privacy	SCP	Secure Copy
TSIG	Transaction Signature Interoperability Group	SAN	Subject Alternative Name or Storage Area Network
TPM	Trusted Platform Module	SaaS	Software as a Service
TCP/IP	Transmission Control Protocol/Internet Protocol	SCAP	Security Content Automation Protocol
TLS	Transport Layer Security	SATCOM	Satellite Communications
TACACS	Terminal Access Controller Access Control System	XACML	eXtensible Access Control Markup Language
USB	Universal Serial Bus	XSS	Cross-Site Scripting
UPS	Uninterruptable Power Supply	XHR	XML Http Request
URL	Universal Resource Locator	XMPP	eXtensible Messaging and Presence
UEFI	Unified Extensible Firmware Interface	VNC	Virtual Network Connection
UDP	User Datagram Protocol	VoIP	Voice over IP
UAC	User Access Control	VPN	Virtual Private Network
UTM	Unified Threat Management	VMFS	Virtual Memory File System
VTPM	Virtual TPM	VM	Virtual Machine
VTC	Video Teleconferencing	VLAN	Virtual Local Area Network
vSAN	Virtual Storage Area Network	VaaS	Voice as a Service
WSDL	Web Services Description Language	WIDS	Wireless Intrusion Detection System
WPA	Wireless Protected Access	WAP	Wireless Access Point
WIPS	Wireless Intrusion Prevention System	WAF	Web Application Firewall

*****