CERTIFICATION GUIDE

CompTIA CASP

What is it?

CompTIA Advanced Security Practitioner (CASP) is the ideal certification for those technical professionals who wish to remain immersed in technology as opposed to managing cybersecurity policy and frameworks.

Why is it different?

CASP is the only hands-on, performance-based certification for practitioners – not managers – at the advanced skill level of cybersecurity. While cybersecurity managers help identify what cybersecurity policies and frameworks could be implemented, CASP-certified professionals figure out how to implement solutions within those policies and frameworks.

About the exam

The CompTIA Advanced Security Practitioner certification validates advanced-level competency in risk management; enterprise security operations and architecture; research and collaboration; and integration of enterprise security.

Successful candidates will have the knowledge required to:

- Conceptualize, engineer, integrate and implement secure solutions across complex enterprise environments to build resilient networks
- 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
- Supervise and respond as team lead to security incidents



Exam #
CAS-003

Release Date
April 2018

Languages
English

CE Required?
Yes

Accreditation
Accredited by ANSI to show compliance with the ISO 17024 Standard. It is also approved by the DoD for Directive 8140/8570.01-M.

What's in this version?

CompTIA is updating CASP in 2018 to continue to address current risks and incident response scenarios inherent with cyber warfare, modern hacking techniques and cloud migration. A sample of changes include:

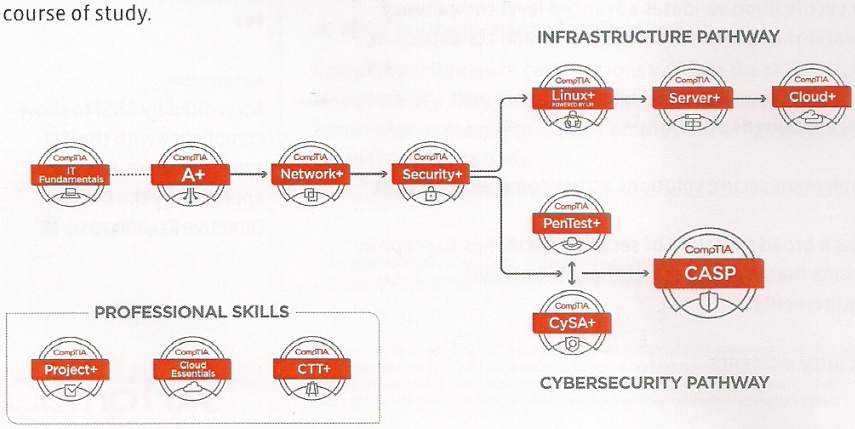
- Enterprise Security domain expanded to include operations and architecture concepts, techniques, and requirements
- More emphasis on analyzing risk through interpreting trend data and anticipating cyber defense needs to meet business goals
- Expanding security control topics to include Mobile and small form factor devices, as well as software vulnerability
- Broader coverage of integrating cloud and virtualization technologies into a secure enterprise architecture
- Inclusion of implementing cryptographic techniques, such as Blockchain- Cryptocurrency and Mobile device encryption

How does CASP Compare to Alternatives?

	CompTIA CASP	CISSP Certified Information Systems Security Professional	GCED	CISM Certified Information Security Manager
Certification	**CASP**	**(ISC)2 Certified Information Systems Security Professional (CISSP)**	**GIAC Certified Enterprise Defender (GCED)**	**ISACA Certified Information Security Manager (CISM)**
Performance-based Questions	Yes	No	No	No
Exam Length	90 questions, 165 minutes	250 questions, 6 hours	115 questions, 3 hours	150 questions, 4 hours
Experience Level	Advanced	Advanced	Advanced	Advanced
Exam Focus	Cybersecurity Practitioner Skills	Cybersecurity Management Skills	Cybersecurity Practitioner Skills	Cybersecurity Management Skills
Pre-requisites	Recommend 10 years of IT administration, including 5 years hands-on, technical security experience.	Documented proof of minimum 5 years full time IT work experience.	None. However, students should be aware of the technical level required for the certification.	Documented proof of minimum 5 years IS work experience in three or more of the job practice analysis areas.

CompTIA Certification Pathway

CompTIA certifications align with the skillsets needed to support and manage IT cybersecurity. Enter where appropriate for you. Consider your experience and existing certifications or course of study.



Top CASP Job Roles

- Security Architect
- Security Engineer
- Application Security Engineer
- Technical Lead Analyst

Technical Areas Covered in the Certification

Risk Management
19%

- Summarize business and industry influences and associated security risks
- Compare and contrast security, privacy policies and procedures based on organizational requirements
- Given a scenario, execute risk mitigation strategies and controls
- Analyze risk metric scenarios to secure the enterprise

Enterprise Security Architecture
25%

- Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements
- Implement security controls for host, mobile and small form factor devices
- Given software vulnerability scenarios, select appropriate security controls

Enterprise Security Operations
20%

- Given a scenario, conduct a security assessment using the appropriate methods
- Analyze a scenario or output, and select the appropriate tool for a security assessment
- Given a scenario, implement incident response and recovery procedures

Technical Integration of Enterprise Security
23%

- Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture
- Integrate cloud and virtualization technologies into a secure enterprise architecture
- Troubleshoot advanced authentication technologies to support enterprise security objectives
- Given a scenario, implement cryptographic techniques

s

Research, Development and Collaboration
13%

- Given a scenario, apply research methods to determine industry trends and their impact to the enterprise
- Implement security activities across the technology life cycle
- Explain the importance of interaction across diverse business units to achieve security goals

Organizations that use CompTIA CASP

- Verizon Telematics
- US Navy
- US Army
- Network Solutions, LLC
- One Source Technologies Inc.
- Booz Allen Hamilton Inc.

Research and Statistics

Job Growth Cybersecurity jobs are predicted to grow more than five times the national average through 2022.[1]

Growing Priority About **8 in 10 managers responsible for security** at their firms across 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years.[2]

Learn with CompTIA

Official CompTIA Content is the only study material exclusively developed by CompTIA for the CompTIA certification candidate; no other content library covers all exam objectives for all certifications. CompTIA eBooks and CertMaster Products have been developed with our Official CompTIA Content to help you prepare for your CompTIA certification exams with confidence. Learners now have everything they need to learn the material and ensure they are prepared for the exam and their career.

Whether you are just starting to prepare and need comprehensive training with CertMaster Learn, need a final review with CertMaster Practice, or need to renew your certification upon expiration with CertMaster CE, CertMaster's online training tools have you covered.

*** What is a Performance Certification?**

CompTIA performance certifications validate the skills associated with a particular job or responsibility. They include simulations that require the test taker to demonstrate multi-step knowledge to complete a task. CompTIA has a higher ratio of these types of questions than any other IT certifying body.

1. Bureau of Labor Statistics, Occupational Outlook 2015
2. CompTIA International Trends in Cybersecurity, April 2016

CompTIA

© 2018 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. 05304A-Jun2018