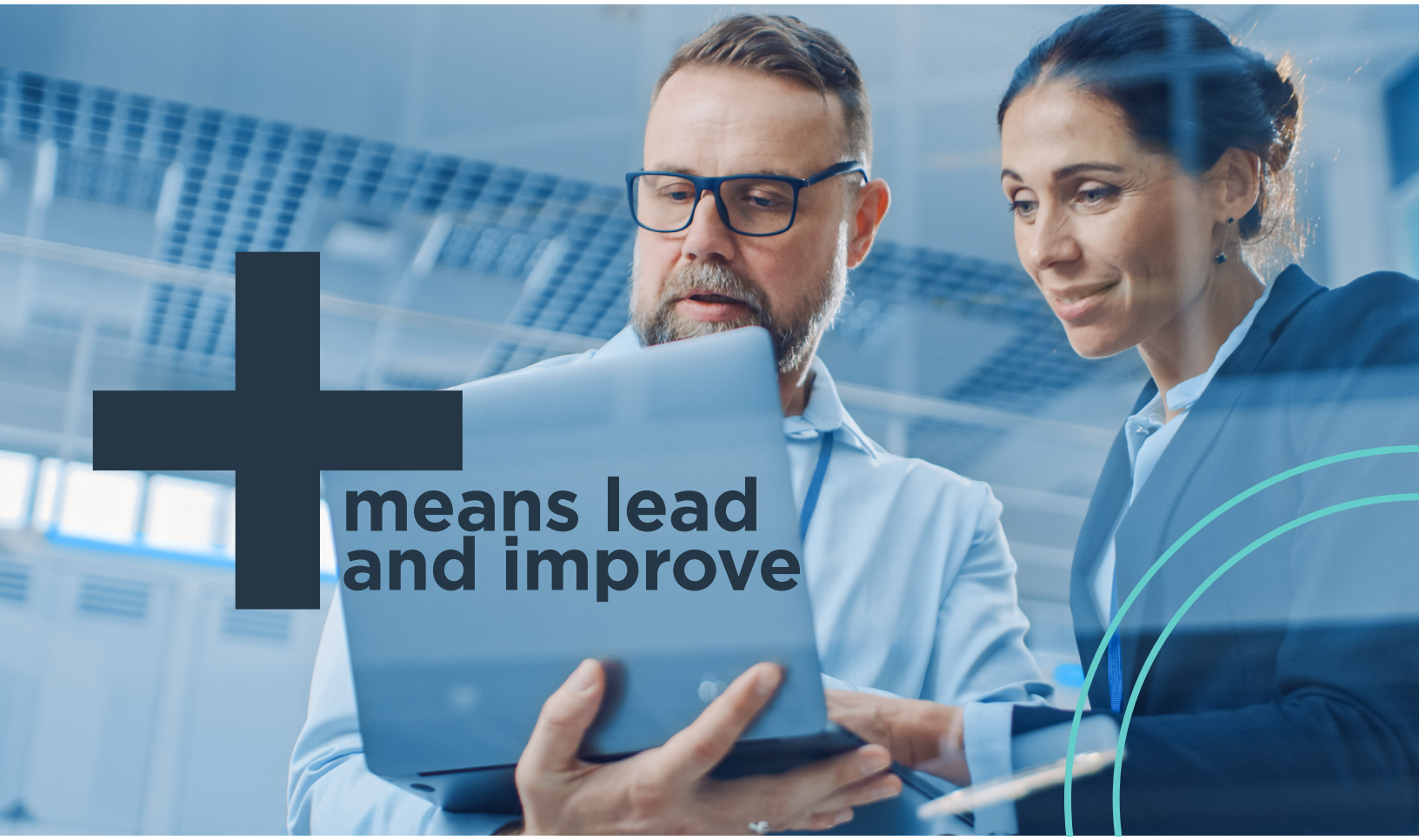
CompTIA



CAS-003 vs CAS-004 Exam Objectives Comparison

As cyberattacks continue to rise globally, organizations are concerned with the lack of qualified senior IT security staff that can skillfully and efficiently design and implement a secure network in either cloud or hybrid environments to combat existing and future threats. Updates to CASP+ qualify advanced skills required of security architects and senior security engineers to effectively design, implement and manage cybersecurity solutions on complex enterprise networks.

CompTIA CASP+ is updated to address the gap between working within complex networks, improving security awareness and decreasing security risks. CASP+004 ensures organizations have advanced technical talent with the latest skills and competencies needed to improve an enterprise's cybersecurity readiness by applying today's best practices with advanced techniques, resulting in innovative, effective and secure solutions that protect the organization and prevent the next attacks.

CASP+ is accredited by ANSI as meeting the ISO/IEC 17024 standard and is approved by U.S. Department of Defense (DoD) to fulfill Directive 8570.01-M/8140 requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA).

Exam Objectives Comparison

The previous CASP+ exam objectives have been updated and made more reflective of cybersecurity architecture and engineering, especially in hybrid and cloud environments. There is a greater emphasis on governance, risk, and compliance skills and how to assess an enterprise's cybersecurity readiness and more focus on leading teams to design, troubleshoot, and implement enterprise-wide cybersecurity solutions.

The following table aligns exam objectives from CAS-003 and CAS- 004 for comparison. Skills are aligned by best match.

CAS-003	CAS-004	RESULTS
2.1 Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements	1.1 Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.	Maps
4.1 Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.	1.2 Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.	Maps
5.2 Given a scenario, implement security activities across the technology life cycle	1.2 Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.	Gap
4.1 Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.	1.3 Given a scenario, integrate software applications securely into an enterprise architecture.	Maps
5.2 Given a scenario, implement security activities across the technology life cycle	1.3 Given a scenario, integrate software applications securely into an enterprise architecture.	Gap
4.1 Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.	1.4 Given a scenario, implement data security techniques for securing enterprise architecture	Maps
4.4 Given a scenario, implement cryptographic techniques	1.4 Given a scenario, implement data security techniques for securing enterprise architecture	Maps
2.2 Analyze a scenario to integrate security controls for host devices to meet security requirements.	1.4 Given a scenario, implement data security techniques for securing enterprise architecture	Maps
2.1 Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements	1.4 Given a scenario, implement data security techniques for securing enterprise architecture	Maps
4.3 Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives	1.5 Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.	Maps
4.2 Given a scenario, integrate cloud and virtualization technologies into a secure enterprise architecture	1.6 Given a set of requirements, implement secure cloud and virtualization solutions.	Maps
n/a	1.7 Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements	New Content
5.1 Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.	1.8 Explain the impact of emerging technologies on enterprise security and privacy	Maps

CAS-003	CAS-004	RESULTS
n/a	2.1 Given a scenario, perform threat management activities	New Content
n/a	2.2 Given a scenario, analyze indicators of compromise and formulate an appropriate response	New Content
n/a	2.3 Given a scenario, perform vulnerability management activities.	New Content
3.2 Analyze a scenario or output, and select the appropriate tool for a security assessment.	2.4 Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools.	Maps
2.4 Given software vulnerability scenarios, select appropriate security controls.	2.5 Given a scenario, analyze vulnerabilities and recommend risk mitigations	Maps
n/a	2.6 Given a scenario, use processes to reduce risk.	New Content
3.3 Given a scenario, implement incident response and recovery procedures	2.7 Given an incident, implement the appropriate response	Maps
n/a	2.8 Explain the importance of forensic concepts	New Content
n/a	2.9 Given a scenario, use forensic analysis tools	New Content
2.3 Analyze a scenario to integrate security controls for mobile and small form factor devices to meet security requirements.	3.1 Given a scenario, apply secure configurations to enterprise mobility.	Maps
2.2 Analyze a scenario to integrate security controls for host devices to meet security requirements	3.1 Given a scenario, apply secure configurations to enterprise mobility.	Maps
2.2 Analyze a scenario to integrate security controls for host devices to meet security requirements	3.2 Given a scenario, configure and implement endpoint security controls.	Maps
n/a	3.3 Explain security considerations impacting specific sectors and operational technologies.	New Content
4.2 Given a scenario, integrate cloud and virtualization technologies into a secure enterprise architecture	3.4 Explain how cloud technology adoption impacts organizational security	Maps
1.1 Summarize business and industry influences and associated security risks.	3.4 Explain how cloud technology adoption impacts organizational security	Maps
4.4 Given a scenario, implement cryptographic techniques	3.5 Given a business requirement, implement the appropriate PKI solution	Maps
4.4 Given a scenario, implement cryptographic techniques	3.6 Given a business requirement, implement the appropriate cryptographic protocols and algorithms.	Maps
4.4 Given a scenario, implement cryptographic techniques	3.7 Given a scenario, troubleshoot issues with cryptographic implementations.	Gap
1.2 Compare and contrast security, privacy policies and procedures based on organizational requirements.	4.1 Given a set of requirements, apply the appropriate risk strategies	Gap
n/a	4.2 Explain the importance of managing and mitigating vendor risk	New Content

CAS-003	CAS-004	RESULTS
1.2 Compare and contrast security, privacy policies and procedures based on organizational requirements.	4.3 Explain compliance frameworks and legal considerations, and their organizational impact	Maps
1.3 Given a scenario, execute risk mitigation strategies and controls	4.3 compliance frameworks and legal considerations, and their organizational impact	Maps
1.3 Given a scenario, execute risk mitigation strategies and controls	4.4 Explain the importance of business continuity and disaster recovery concepts.	Maps
1.4 Analyze risk metric scenarios to secure the enterprise	4.4 Explain the importance of business continuity and disaster recovery concepts.	Maps