CompTIA SecurityX

CompTIA Advanced Security Practitioner (CASP+) will be re-branded to SecurityX with the next exam version CAS-005. This name change will not affect the status of current CASP+ certification holders and those with an active CASP+ certification will receive a SecurityX certification.

The certification will continue to:

- Validate job tasks performed by a security professional with 10 years of IT experience and 5 years of security experience
- Be designed around the tasks performed by senior security engineer and security architect roles
- Be a natural progression from the job roles aligned to Security+

The certification validates that successful candidates have the knowledge and skills to:

- Architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise.
- Use automation, monitoring, detection, and incident response to proactively support ongoing security operations in an enterprise environment.
- Apply security practices to cloud, on-premises, and hybrid environments.
- Consider cryptographic technologies and techniques, as well as the impact of emerging trends (e.g., artificial intelligence) on information security.
- Use the appropriate governance, compliance, risk management, and threat modeling strategies throughout the enterprise.

Exam Objectives Comparison

The following table aligns exam objectives from CAS-005 and CAS-004 for comparison. Skills are aligned by best match.

CAS-005		CAS-004		Gap Indicator
1.1	Given a set of organizational security requirements, implement the appropriate governance components.	n/a		New content
1.2	Given a set of organizational security requirements, perform risk management activities.	4.1	Given a set of requirements, apply the appropriate risk strategies.	Maps
1.2	Given a set of organizational security requirements, perform risk management activities.	4.2	Explain the importance of managing and mitigating vendor risk.	Gap
1.3	Explain how compliance affects information security strategies.	4.3	Explain compliance frameworks and legal considerations, and their organizational impact.	Maps
1.4	Given a scenario, perform threat modeling activities.	n/a		New content
1.5	Summarize the information security challenges associated with artificial intelligence (AI) adoption.	n/a		New content
2.1	Given a scenario, analyze requirements to design resilient systems.	4.4	Explain the importance of business continuity and disaster recovery concepts.	Gap
2.1	Given a scenario, analyze requirements to design resilient systems.	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
2.1	Given a scenario, analyze requirements to design resilient systems.	1.2	Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.	Maps
2.2	Given a scenario, implement security in the early stages of the systems life cycle and throughout subsequent stages.	1.3	Given a scenario, integrate software applications securely into an enterprise architecture.	Maps
2.3	Given a scenario, integrate appropriate controls in the design of a secure architecture.	1.2	Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.	Maps
2.3	Given a scenario, integrate appropriate controls in the design of a secure architecture.	1.4	Given a scenario, implement data security techniques for securing enterprise architecture.	Maps

CAS-005		CAS-004		Gap Indicator
2.3	Given a scenario, integrate appropriate controls in the design of a secure architecture.	1.4	Given a scenario, implement data security techniques for securing enterprise architecture.	Maps
2.3	Given a scenario, integrate appropriate controls in the design of a secure architecture.	2.2	Given a scenario, analyze indicators of compromise and formulate an appropriate response.	Maps
2.4	Given a scenario, apply security concepts to the design of access, authentication, and authorization systems.	1.5	Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.	Maps
2.4	Given a scenario, apply security concepts to the design of access, authentication, and authorization systems.	3.5	Given a business requirement, implement the appropriate PKI solution.	Maps
2.5	Given a scenario, securely implement cloud capabilities in an enterprise environment.	n/a		New content
2.6	Given a scenario, integrate Zero Trust concepts into system architecture design.	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
3.1	Given a scenario, troubleshoot common issues with identity and access management (IAM) components in an enterprise environment.	1.5	Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.	Maps
3.2	Given a scenario, analyze requirements to enhance the security of endpoints and servers.	3.2	Given a scenario, configure and implement endpoint security controls.	Gap
3.3	Given a scenario, troubleshoot complex network infrastructure security issues.	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
3.4	Given a scenario, implement hardware security technologies and techniques.	3.2	Given a scenario, configure and implement endpoint security controls.	Maps
3.5	Given a set of requirements, secure specialized and legacy systems against threats.	3.3	Explain security considerations impacting specific sectors and operational technologies.	Gap
3.6	Given a scenario, use automation to secure the enterprise.	n/a		New content
3.7	Explain the importance of advanced cryptographic concepts.	n/a		New content

CAS-005		CAS-004		Gap Indicator
3.8	Given a scenario, apply the appropriate cryptographic use case and/or technique.	3.6	Given a business requirement, implement the appropriate cryptographic protocols and algorithms.	Maps
3.8	Given a scenario, apply the appropriate cryptographic use case and/or technique.	3.7	Given a scenario, troubleshoot issues with cryptographic implementations.	Maps
4.1	Given a scenario, analyze data to enable monitoring and response activities.	n/a		New content
4.2	Given a scenario, analyze vulnerabilities and attacks, and recommend solutions to reduce the attack surface.	2.5	Given a scenario, analyze vulnerabilities and recommend risk mitigations.	Maps
4.2	Given a scenario, analyze vulnerabilities and attacks, and recommend solutions to reduce the attack surface.	2.6	Given a scenario, use processes to reduce risk.	Gap
4.3	Given a scenario, apply threat-hunting and threat intelligence concepts.	n/a		New content
4.4	Given a scenario, analyze data and artifacts in support of incident response activities.	2.7	Given an incident, implement the appropriate response.	Gap
4.4	Given a scenario, analyze data and artifacts in support of incident response activities.	2.8	Explain the importance of forensic concepts.	Gap
4.4	Given a scenario, analyze data and artifacts in support of incident response activities.	2.2	Given a scenario, analyze indicators of compromise and formulate an appropriate response.	Gap

CompTIA