Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

CASP+ Certification Training Course

Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

Overview

The CompTIA Advanced Security Practitioner (CASP+) certification is an international, vendor-neutral exam that proves competency in enterprise security; risk management; research and analysis; and integration of computing, communications, and business disciplines. The exam covers the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments. It involves applying 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 was accredited by the International Organization for Standardization (ISO) and the American National Standards Institute (ANSI).

Advanced security professional's certification provided by CompTIA as the names says is mainly not only for the professionals but also to for the managers. The course helps to understand the cyber security policies and frameworks and how to implement them in an organisation.

DOMAINS

- Enterprise Security
- Risk Management and Incident Response
- Research and Analysis
- Integration of Computing, Communications and Business Disciplines
- Technical Integration of Enterprise Components

1. Enterprise Security

- Given a scenario, select appropriate cryptographic concepts and techniques.
- Explain the security implications associated with enterprise storage.
- Given a scenario, analyse network and security components, concepts and architectures.
- Given a scenario, select and troubleshoot security controls for hosts.
- Differentiate application vulnerabilities and select appropriate security controls.

2. Risk Management and Incident Response

- Interpret business and industry influences and explain associated security risks.
- Given a scenario, execute risk mitigation planning, strategies and controls.
- Compare and contrast security, privacy policies and procedures based on organizational requirements.
- Given a scenario, conduct incident response and recovery procedures.

Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

3. Research, Analysis and Assessment

- Apply research methods to determine industry trends and impact to the enterprise.
- Analyse scenarios to secure the enterprise.
- Given a scenario, select methods or tools appropriate to conduct an assessment and analyse results.

4. Integration of Computing, Communications and Business Disciplines

- Given a scenario, facilitate collaboration across diverse business units to achieve security goals
- Given a scenario, select the appropriate control to secure communications and collaboration solutions.
- Implement security activities across the technology life cycle.

5. Technical Integration of Enterprise Components

- Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.
- Given a scenario, integrate advanced authentication and authorization technologies to support enterprise objectives.