

CompTIA Advanced Security Practitioner (CASP) Certification



Course Outline

Domain 1. Enterprise Security

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

Domain 2. Risk Management and Incident Response

- Interpret business and industry influences and explain associated security risks
- Execute risk mitigation planning, strategies and controls
- Compare and contrast security, privacy policies and procedures based on organizational requirements
- Conduct incident response and recovery procedures

Domain 3. Research, Analysis and Assessment

- Apply research methods to determine industry trends and impact to the enterprise
- Analyze scenarios to secure the enterprise
- Select methods or tools appropriate to conduct an assessment and analyze results

Domain 4. Integration of Computing, Communications and Business Disciplines

- Facilitate collaboration across diverse business units to achieve security goals
- Select the appropriate control to secure communications and collaboration solutions
- Implement security activities across the technology life cycle

Domain 5. Technical Integration of Enterprise Components

- Integrate hosts, storage, networks and applications into a secure enterprise architecture
- Integrate advanced authentication and authorization technologies to support enterprise objectives