CompTIA CASP (Advanced Security Practitioner)

Course Length: 5 days (virtual)

Click here to view the current class schedule!

Overview:

The CompTIA Advanced Security Practitioner (CASP) Certification is a vendor-neutral credential. The CASP exam is an internationally targeted validation of advanced-level security skills and knowledge. While there is no required prerequisite, the CASP certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, "hands-on" focus at the enterprise level.

The CASP exam will certify that the successful candidate has the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments. The candidate will 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, analyzes risk impact and respond to security incidents.

Exam: CAS-002

The CompTIA Advanced Security Practitioner (CASP) Certification is aimed at an IT security professional who has:

- A minimum of 10 years experience in IT administration including at least 5 years of hands-on technical security experience.

1.0 Enterprise Security

1.1 Given a scenario, select appropriate cryptographic concepts and techniques.

- Techniques
- Concepts
- Implementations

1.2 Explain the security implications associated with enterprise storage

- Storage types
- Storage protocols
- Secure storage management

1.3 Given a scenario, analyze network and security components, concepts and architectures

- Advanced network design (wired/wireless)
- Security devices
- Virtual networking and security components
- Complex network security solutions for data flow
- Secure configuration and baselining of networking and security components
- Software defined networking
- Cloud managed networks

- Network management and monitoring tools
- Advanced configuration of routers, switches and other network devices
- Security zones
- Network access control
- Operational and consumer network enabled devices
- Critical infrastructure/Supervisory Control and Data Acquisition (SCADA)/Industrial Control Systems (ICS)

1.4 Given a scenario, select and troubleshoot security controls for hosts

- Trusted OS (e.g. how and when to use it)
- End point security software
- Host hardening
- Security advantages and disadvantages of virtualizing servers
- Cloud augmented security services
- Boot loader protections
- Vulnerabilities associated with co-mingling of hosts with different security requirements
- Virtual Desktop Infrastructure (VDI)
- Terminal services/application delivery services
- TPM
- VTPM
- HSM

1.5 Differentiate application vulnerabilities and select appropriate security controls

- Web application security design considerations
- Specific application issues
- Application sandboxing
- Application security frameworks
- Secure coding standards
- Database Activity Monitor (DAM)
- Web Application Firewalls (WAF)
- Client-side processing vs. server-side processing

2.0 Risk Management and Incident Response

2.1 Interpret business and industry influences and explain associated security risks

- Risk management of new products, new technologies and user behaviors
- New or changing business models/strategies
- Security concerns of integrating diverse industries
- Ensuring third party providers have requisite levels of information security
- Internal and external influences
- Impact of de-perimeterization (e.g. constantly changing network boundary)

2.2 Given a scenario, execute risk mitigation planning, strategies and controls

- Classify information types into levels of CIA based on organization/industry
- Incorporate stakeholder input into CIA decisions
- Implement technical controls based on CIA requirements and policies of the organization

- Determine aggregate score of CIA
- Extreme scenario planning/worst case scenario
- Determine minimum required security controls based on aggregate score
- Conduct system specific risk analysis
- Make risk determination
- Recommend which strategy should be applied based on risk appetite
- Risk management processes
- Enterprise Security Architecture frameworks
- Continuous improvement/monitoring
- Business Continuity Planning
- IT Governance

2.3 Compare and contrast security, privacy policies and procedures based on organizational requirements

- Policy development and updates in light of new business, technology, risks and environment changes
- Process/procedure development and updates in light of policy, environment and business changes
- Support legal compliance and advocacy by partnering with HR, legal, management and other entities
- Use common business documents to support security
- Use general privacy principles for sensitive information (PII)
- Support the development of policies

2.4 Given a scenario, conduct incident response and recovery procedures

- E-Discovery
- Data breach
- Design systems to facilitate incident response
- Incident and emergency response

3.0 Research, Analysis and Assessment

3.1 Apply research methods to determine industry trends and impact to the enterprise

- Perform ongoing research
- Situational awareness
- Research security implications of new business tools
- Global IA industry/community
- Research security requirements for contracts

3.2 Analyze scenarios to secure the enterprise

- Create benchmarks and compare to baselines
- Prototype and test multiple solutions
- Cost benefit analysis
- Metrics collection and analysis
- Analyze and interpret trend data to anticipate cyber defense needs
- Review effectiveness of existing security controls
- Reverse engineer/deconstruct existing solutions
- Analyze security solution attributes to ensure they meet business needs
- Conduct a lessons-learned/after-action report

- Use judgment to solve difficult problems that do not have a best solution

3.3 Given a scenario, select methods or tools appropriate to conduct an assessment and analyze results

- Tool type
- Methods

4.0 Integration of Computing, Communications and Business Disciplines

4.1 Given a scenario, facilitate collaboration across diverse business units to achieve security goals

- Interpreting security requirements and goals to communicate with stakeholders from other disciplines
- Provide objective guidance and impartial recommendations to staff and senior management on security processes and controls
- Establish effective collaboration within teams to implement secure solutions
- IT governance

4.2 Given a scenario, select the appropriate control to secure communications and collaboration solutions

- Security of unified collaboration tools
- Remote access
- Mobile device management
- Over-the-air technologies concerns

4.3 Implement security activities across the technology life cycle

- End-to-end solution ownership
- Systems Development Life Cycle
- Adapt solutions to address emerging threats and security trends
- Asset management (inventory control)

5.0 Technical Integration of Enterprise Components

5.1 Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture

- Secure data flows to meet changing business needs
- Standards
- Interoperability issues
- Technical deployment models (Outsourcing/insourcing/managed services/partnership)
- Logical deployment diagram and corresponding physical deployment diagram of all relevant devices
- Secure infrastructure design (e.g. decide where to place certain devices/applications)
- Storage integration (security considerations)
- Enterprise application integration enablers

5.2 Given a scenario, integrate advanced authentication and authorization technologies to support enterprise objectives

- Authentication
- Authorization

- Attestation
- Identity propagation
- Federation
- Advanced trust models