

CompTIA Advanced Security Practitioner IN-CASP



| | |
|-----------------------------|---|
| Course Name | CompTIA Advanced Security Practitioner |
| Course Code | IN-CASP |
| Course Duration | 5 Days |
| Course Structure | Instructor-Led |
| Course Overview | <p>The CompTIA Advanced Security Practitioner (CASP) course is a 5-day training course aimed at IT professionals with at least 10 years of experience in enterprise IT Security, who intend on writing the CompTIA CAS-003 exam. In this course, delegates will expand on their knowledge of information security to apply more advanced principles that will keep their organization safe from the many ways it can be threatened.</p> <p>Delegates 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, support IT governance and risk management, architect security for hosts, networks, and software, respond to security incidents and more.</p> |
| Audience Profile | <p>This course is designed for IT professionals in the cybersecurity industry whose primary job responsibility is to secure complex enterprise environments. The target student should have real-world experience with the technical administration of these enterprise environments. The target audience includes the following:</p> <ul style="list-style-type: none"> • Cyber Security/IS Professionals • Information Security Analysts • Security Architects • IT Specialist • Cybersecurity Risk Managers • Cybersecurity Risk Analysts |
| Course Prerequisites | <p>Before attending this course, delegates need to have knowledge of Information Security concepts. This includes, but is not limited to:</p> <ul style="list-style-type: none"> • Knowledge of identity and access management (IAM) concepts and common implementations, such as authentication factors and directory services |

| | |
|-------------------------------------|---|
| | <ul style="list-style-type: none"> • Knowledge of cryptographic concepts and common implementations, such as Secure Sockets Layer/Transport Layer Security (SSL/TLS) and public key infrastructure (PKI) • Knowledge of computer networking concepts and implementations, such as the TCP/IP model and configuration of routers and switches • Knowledge of common security technologies used to safeguard the enterprise, such as anti-malware solutions, firewalls, and VPNs |
| <p>Course Outcome</p> | <p>In this course, delegates will analyse and apply advanced security concepts, principles, and implementations that contribute to enterprise-level security. Upon successful completion of this course, delegates will be able to:</p> <ul style="list-style-type: none"> • Leverage collaboration tools and technology to support enterprise security • Use research and analysis to secure the enterprise • Integrate advanced authentication and authorization techniques • Implement cryptographic techniques • Implement security controls for hosts • Implement security controls for mobile devices • Implement network security • Implement security in the systems and software development lifecycle • Integrate hosts, storage, networks, applications, virtual environments, and cloud technologies in a secure enterprise architecture • Conduct security assessments • Respond to and recover from security incidents |
| <p>Assessment/Evaluation</p> | <p>This course will prepare delegates to take the CompTIA CASP CAS-003 Exam.</p> <p>Successfully passing this exam will result in the attainment of the CompTIA Advanced Security Practitioner Certification and Certificate of Attendance issued by IT-IQ Botswana</p> |

| Course Details | |
|-----------------------|---|
| Topic | Topic 1: Supporting IT Governance and Risk Management Topic 2: Leveraging Collaboration to Support Security Topic 3: Using Research and Analysis to Secure the Enterprise Topic 4: Integrating Advanced Authentication and Authorization Techniques Topic 5: Implementing Cryptographic Techniques Topic 6: Implementing Security Controls for Hosts Topic 7: Implementing Security Controls for Mobile Devices Topic 8: Implementing Network Security |