# COURSE OVERVIEW

**Course Name:**
(CAS-004) CompTIA Advanced Security Practitioner (CASP)+

**COURSE DURATION:** 5 Day

**Gauteng:**
3rd Floor, 34 Whitely Road
Melrose Arch
Johannesburg
2196

**Gauteng:**
192 on Bram
192 Bram Fischer Drive
Ferndale, Randburg
Johannesburg
2160

**Cape Town:**
3rd Floor, Thomas Pattullo Building
19 Jan Smuts St
Cape Town
8000

**Durban:**
9 Mountview Close
Broadlands
Mount Edgecombe
Durban
4302

☎ 087 941 5764
✉ sales@impactful.co.za
🌐 impactful.co.za

## INTRODUCTION

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-004 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.

Delegates will apply critical thinking and judgment a cross abroad 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.

## DELIVERY METHOD

Our courses have flexible delivery options:

- In-person classroom training at the Impactful training facilities
  - Johannesburg, Durban, Cape Town
- Virtual instructor-led training
- Nationally: on-site at the client

IMPACTFUL
Powered by LRMG

## INTENDED AUDIENCE

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:

- Cybersecurity/IS Professionals
- Information Security Analysts
- Security Architects
- IT Specialist
- Cybersecurity Risk Managers

## PREREQUISITES

Before attending this course, delegates need to have knowledge of Information Security concepts. This includes, but is not limited to:

- Knowledge of identity and access management (IAM) concepts and common implementations, such as authentication factors and directory services
- 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

It is highly recommended that delegates attending this course have a minimum of 10years' experience in IT administration, including at least 5 years of hands-on technical security experience.

## COURSE OBJECTIVES

- 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:
- 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 Manage packages
- Configure the GUI

## COURSE CONTENT

Lesson 1: Perform Risk Management Activities•
Topic 1A: Explain Risk Assessment Methods
•Topic 1B: Summarize the Risk Lifecycle
•Topic 1C: Assess & Mitigate Vendor Risk

Lesson 2: Summarizing Governance & Compliance Strategies
•Topic 2A: Meet Cloud Identifying Critical Data Assets
•Topic 2B: Design Compare and Contrast Regulation, Accreditation, and Standards
•Topic2C: Explain Legal Considerations & Contract Types

Lesson 3: Implementing Business Continuity & Disaster Recovery
•Topic 3A: Explain the Role of Business Impact Analysis
•Topic 3B: Assess Disaster Recovery Plans
•Topic 3C: Explain Testing and Readiness Activities

Lesson 4: Identifying Infrastructure Services
•Topic 4A: Explain Critical Network Services
•Topic 4B: Explain Defensible Network Design
•Topic 4C: Implement Durable Infrastructures

Lesson 5: Performing Software Integration
•Topic 5A: Explain Secure Integration Activities
•Topic 5B: Assess Software Development Activities
•Topic 5C: Analyze Access Control Models & Best Practices
•Topic 5D: Analyze Development Models & Best Practices

Lesson 6: Explain Virtualization, Cloud, and Emerging Technology
•Topic 6A: Explain Virtualization and Cloud Technology
•Topic 6B: Explain Emerging Technologies Lesson 7: Exploring Secure Configurations and System Hardening
•Topic 7A: Analyze Enterprise Mobility Protections
•Topic 7B: Implement Endpoint Protection

Lesson 8: Understanding Security Considerations of Cloud and Specialized Platforms
•Topic 8A: Understand Impacts of Cloud Technology Adoption
•Topic 8B: Explain Security Concerns for Sector Specific Technologies

Lesson 9: Implementing Cryptography
•Topic 9A: Implementing Hashing and Symmetric Algorithms
•Topic 9B: Implementing Appropriate Asymmetric Algorithms and Protocols

Lesson 10: Implementing Public Key Infrastructure (PKI)
•Topic 10A: Analyze Objectives of Cryptography and Public Key Infrastructure (PKI)
•Topic 10B: Implementing Appropriate PKI Solutions

Lesson 11: Understanding Threat and Vulnerability Management Activities
•Topic 11A: Explore Threat and Vulnerability Management Concepts Activities
•Topic 11B: Explain Vulnerability and Penetration Test Methods
•Topic 11C: Explain Technologies Designed to Reduce Risk

Lesson 12: Developing Incident Response Capabilities
•Topic 12A: Analyzing and Mitigating Vulnerabilities
•Topic 12B: Identifying and Responding to Indicators of Compromise
•Topic 12C: Exploring Digital Forensic Concepts

## ASSOCIATED CERTIFICATION AND EXAM

This course will prepare delegates to write the CompTIA CASP+ (**CAS-004**) exam.