

Certified Information Systems Security Professional (CISSP)

Duration: 5 Days

Language: en

Course Code: PI1 - 134

Objective

Upon completion of this course, participants will be able to:

- Provide a comprehensive understanding of the eight CISSP CBK domains.
- Develop skills in identifying and mitigating security risks.
- Equip participants with knowledge of best practices in information security management.
- Prepare participants for the CISSP certification exam.
- Enhance participants' ability to design, implement, and manage secure information systems.

Audience

This course is ideal for IT professionals and security practitioners responsible for managing and protecting an organisation’s information systems. It is particularly beneficial for:

- Information security analysts
- Network security engineers
- Security consultants
- IT managers
- Systems administrators
- Security auditors and architects
- Professionals looking to advance their careers in cybersecurity

Training Methodology

The CISSP training course adopts a blended learning approach to ensure participants can apply theoretical and practical knowledge. It includes lectures, case studies, real-world scenarios, and hands-on labs. Interactive discussions and group activities are integrated into each session to encourage collaborative learning and knowledge-sharing among participants. Simulated cybersecurity exercises and exams provide participants practical experience managing security incidents and implementing protective measures.

Participants can also access online resources, including sample questions, study guides, and mock exams to support self-paced learning and exam preparation.

Summary

The Certified Information Systems Security Professional (CISSP) training course is a comprehensive programme to equip IT professionals with advanced cybersecurity skills. As one of the most recognised and valued certifications globally, CISSP is essential for professionals aspiring to build and advance their careers in information security. The course covers various security practices, policies, and procedures to secure an organisation's information systems, including access control, cryptography, disaster recovery, and security management.

This training is structured to provide a thorough understanding of the eight domains of the

CISSP Common Body of Knowledge (CBK), which are key to the certification. Each domain delves into critical topics like software development security, risk management, and network security to ensure participants are well-prepared to handle real-world security challenges.

This course combines theoretical knowledge with practical insights and is designed for those who aspire to be security consultants, IT managers, or security auditors. Through case studies, simulations, and hands-on exercises, participants will gain experience assessing and mitigating risks, implementing security controls, and understanding the legal and regulatory frameworks governing information security.

At the end of the course, participants will have the necessary tools to pass the CISSP certification exam, positioning themselves as leaders in the ever-evolving cybersecurity landscape. The CISSP credential enhances career prospects and ensures that professionals can protect their organisations against modern security threats.

Course Content & Outline

Section 1: Introduction to CISSP and Cybersecurity Fundamentals

- Overview of CISSP certification and its importance
- The role of cybersecurity in today’s IT environment
- Introduction to the eight domains of the CISSP CBK

Section 2: Security and Risk Management

- Security governance principles
- Compliance and legal issues in cybersecurity
- Risk management frameworks and methodologies
- Business continuity and disaster recovery planning

Section 3: Asset Security and Security Architecture

- Classification and protection of assets
- Security models and frameworks
- Designing and implementing secure architectures

Section 4: Communication and Network Security

- Network protocols and services

- Securing network infrastructure
- Virtual private networks (VPNs) and firewalls
- Intrusion detection and prevention systems

Section 5: Identity and Access Management (IAM)

- Access control models and methods
- Authentication and authorisation techniques
- Identity as a service (IDaaS)
- Managing user lifecycle and privileges

Section 6: Security Assessment and Testing

- Types of security assessments
- Vulnerability management
- Penetration testing methodologies
- Incident response and forensic investigation

Section 7: Security Operations

- Security operations management
- Logging and monitoring activities
- Security event management systems
- Incident management and disaster recovery

Section 8: Software Development Security

- Secure coding practices
- Software development life cycle (SDLC) and security
- Application security threats and mitigations
- Testing and auditing software for vulnerabilities



Certificate Description

Upon successful completion of this training course, delegates will be awarded a Holistique Training Certificate of Completion. For those who attend and complete the online training course, a Holistique Training e-Certificate will be provided.

Holistique Training Certificates are accredited by the British Assessment Council (BAC) and The CPD Certification Service (CPD), and are certified under ISO 9001, ISO 21001, and ISO 29993 standards.

CPD credits for this course are granted by our Certificates and will be reflected on the Holistique Training Certificate of Completion. In accordance with the standards of The CPD Certification Service, one CPD credit is awarded per hour of course attendance. A maximum of 50 CPD credits can be claimed for any single course we currently offer.

Categories

IT & Computer Application, Technology

Tags

Information Security Management, Information Systems Security

Related Articles

What is Information Technology? A Comprehensive Guide to Modern Tech and Applications