Certified Information System Security Professional (CISSP)

Duration: 5 days
Audience: Professionnel TI

Who is this training for?

- Security Consultant • Security Analyst
- Security Manager
- Security System Engineer
- Information Security Director
- IT Director or Manager
- Security Auditor
- Security Director
- Security Architect
- Network Architect

Training objectives

- Understand risk management concepts, security policies, and compliance frameworks
- Protect the organization's information and assets
- Design and implement robust security solutions
- Ensure network and communications security
- Manage identities and access to ensure that only authorized individuals have access to resources
- Assess and test security systems to identify vulnerabilities
- Manage Everyday Security Operations
- Embed security practices into the software development lifecycle

Summary

By participating in this intensive, five-day knowledge-based training, you will be prepared by an expert to design, implement, and manage information security programs. This training is designed to help you prepare for the CISSP exam.

Course outline

Module 1: Security and Risk Management

- Understand and apply the concepts of confidentiality, integrity and availability
- Apply security governance principles
- Compliance
- Understand the legal and regulatory issues that relate to information security in a global context
- Develop and implement a documented security policy, standards, Procedures and guidelines
- Understand business continuity requirements
- Contribute to personnel security policies
- Understand and apply risk management concepts
- Understand and apply threat modeling
- Integrate security risk factors into procurement strategy and practice
- Establish and manage security education, training, and awareness

Module 2: Asset Security

- Classify Information and Support Resources
- Determine and Maintain Property
- Protect Privacy
- Ensure Appropriate Retention
- Determine Data Security Controls
- Establish Handling Requirements

Module 3: Security Engineering

- Implement and Manage an Engineering Lifecycle Using Security Design Principles
-

Understand the Fundamental Concepts of Security Models

- Select Controls and countermeasures based on information systems security standards
- Understand information systems security capabilities
- Assess and mitigate vulnerabilities in security architectures, designs, and solution elements
- Assess and mitigate vulnerabilities in web-based systems
- Assess and mitigate vulnerabilities in mobile systems
- Assess and mitigate vulnerabilities in embedded devices and cyber-physical systems
- Apply Cryptography
- Apply Secure Principles to Site and Facility Design
- Facility Security Design and Implementation

Module 4: Communications and Network Security

- Apply Secure Design Principles to Network Architecture
- Secure Network Components
- Design and Establish Secure Communication Channels
- Prevent or Mitigate Network Attacks

Module 5: Identity and Access Management

- Control Physical and Logical Access to Resources
- Manage Identification and Authentication of People and Devices
- Onboard Identity as a Service (IDaaS)
- Third-Party Identity Services Integration
- Implement and Manage Authorization Mechanisms
- Prevent or Mitigate Access Control Attacks
- Manage the Identity and Access Provisioning Lifecycle

Module 6: Security Assessment and Testing

- Design and validate assessment and testing strategies
-

Perform security control testing

- Collect security process data
- Conduct or facilitate internal and external audits

Module 7: Security Operations

- Understand and support investigations
- Understand requirements for investigation types
- Lead logging and monitoring activities
- Secure resource provisioning through Configuration Management
- Understand and apply fundamental concepts of security operations
- Employ asset protection techniques
- Incident response
- Operate and maintain preventive measures
- Implement and support patching and vulnerability management
- Participate in and understand change management processes
- Implement recovery strategies
- Implement disaster recovery processes
- Disaster Testing
- Participate in Business Continuity Planning
- Implement and Manage Physical Security
- Participate in Personnel Security

Module 8: Software Development Security

- Understand and Apply Security in the Software Development Lifecycle
- Apply Security Controls in the Development Environment
- Evaluate Software Security Effectiveness
- Evaluate Software Acquisition Security

Approach and methodology

Structured presentations to cover all areas of the CISSP and to understand the key concepts. Presentation of frameworks, standards and best practices in information security in order to reinforce theoretical knowledge. Case studies and concrete examples to facilitate the application of the concepts in real professional contexts. Review exercises and exam-style questions to help prepare for certification. Exchanges and clarification with the expert trainer to deepen understanding and answer questions.

Prerequisites

Five years of experience in IT infrastructure and cybersecurity

Recommendations

This training is intended for experienced professionals in cybersecurity or IT infrastructure who wish to prepare for the CISSP certification. It is recommended to have a solid experience (about 5 years) in at least one or more fields related to information systems security in order to maximize learning. A prior review of the fundamental concepts of information security (risk management, networks, architecture, etc.) promotes better assimilation of content. The implementation of a personal study plan and regular practice (readings, exercises, mock exams) are strongly suggested to optimize exam preparation. It is advisable to complete the training with reading and continuous practice in order to deepen the concepts and consolidate the skills acquired

Certifications

CISSP Exam Preparation