Certified Information Systems Security Professional – CISSP

Description

Expand your knowledge of information security

This course teaches the concepts of information security and industry best practices, covering the eight domains of the official CISSP CBK (Common Body of Knowledge).
You will gain knowledge in information security that will enhance your ability to successfully implement and manage security programs in any organization or governmental entity.

We prepare you for the CISSP exam: Certified Information Systems Security Professional

This 5-day training effectively prepares you for the CISSP (Certified Information Systems Security Professional) exam. This course will cover, among other topics, security and risk management, security engineering, and the evaluation of the effectiveness of existing security measures.

Course Content
Module 1: Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulation, Business Continuity)

- Understand and apply the concepts of confidentiality, integrity, and availability
- Apply security governance principles
- Compliance
- Understand legal and regulatory issues that relate to information security in a global context
- Develop and implement documented security policies, 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 acquisition strategy and practice
- Establish and manage security education, training, and awareness

Module 2: Asset Security (Protecting Security of Assets)

- Classify information and support resources
- Determine and maintain ownership

- Protect privacy
- Ensure proper retention
- Determine data security controls
- Establish handling requirements

Module 3: Security Engineering (Engineering and Management of Security)

- Implement and manage an engineering lifecycle using security design principles
- Understand fundamental concepts of security models
- Select controls and countermeasures based on information security standards
- Understand information system security capabilities
- Assess and mitigate vulnerabilities in security architectures, designs, and solution elements
- Assess and mitigate vulnerabilities in web 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
- Design and implement facility security

Module 4: Communications and Network Security (Designing and Protecting 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 (Access Control and Identity Management)

- Control physical and logical access to assets
- Manage identification and authentication of people and devices
- Integrate Identity as a Service (IDaaS)
- Integrate third-party identity services
- Implement and manage authorization mechanisms
- Prevent or mitigate access control attacks
- Manage the identity and access provisioning lifecycle

Module 6: Security Assessment and Testing (Designing, Performing, and Analyzing Security 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 (e.g., Foundational Concepts, Investigations, Incident Management, Disaster Recovery)

- Understand and support investigations
- Understand the requirements for investigation types
- Conduct logging and monitoring activities
- Secure resource provisioning through configuration management
- Understand and apply foundational security operations concepts
- Employ resource protection techniques
- Incident response

- Operate and maintain preventive measures
- Implement and support patch and vulnerability management
- Participate and understand change management processes
- Implement recovery strategies
- Implement disaster recovery processes
- Test disaster recovery plans
- Participate in business continuity planning
- Implement and manage physical security
- Participate in personnel security

Module 8: Software Development Security (Understanding, Applying, and Enforcing Software Security)

- Understand and apply security in the software development lifecycle
- Apply security controls in the development environment
- Assess the effectiveness of software security
- Assess the security of software acquisition

Documentation

- Digital courseware included

Exam

- This course prepares you to the CISSP: Certified Information Systems Security Professional exam. If you wish to take this exam, please contact our secretariat who will let you know the cost of the exam and will take care of all the necessary administrative procedures for you

Participant profiles

- Anyone whose position requires CISSP certification
- Individuals who want to advance within their current computer security careers or migrate to a related career

Prerequisites

- Minimum of five years of experience working in IT Infrastructures and Cybersecurity

Objectives

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Description
Certified Information Systems Security Professional training - CISSP
Niveau
Avancé
Classroom Registration Price (CHF)
4900
Virtual Classroom Registration Price (CHF)

4650
Duration (in Days)
5
Reference
ISC-CISSP