Chief Information Security Officer (CISO)

Date and duration

Training code : SEC24EN
Duration : 4,5 days
Nombre d'heures : 31 heures

Training with certification

PECB Certified Chief Information Security Officer

Body

The Chief Information Security Officer (CISO), or **Responsable de la Sécurité des Systèmes d'Information (RSSI)**, plays a critical role in protecting an organization's data. As the guarantor of confidentiality, integrity, and availability of information, the CISO defines security policies, manages risks, ensures compliance (such as GDPR), raises employee awareness, and oversees incident management. A true **technical, managerial, and legal expert**, the CISO is also able to communicate effectively at all levels of the organization.
The **PECB CISO training** is an intensive program designed to provide you with the essential skills to lead your organization's information security. You will gain in-depth expertise in key areas such as **designing and implementing effective security programs, managing risks**, and ensuring compliance with standards and regulations (GDPR, ISO/IEC 27001, etc.). You will also master the implementation of robust security measures, incident management, and security awareness training for your teams.
At the end of this course, you will be ready to take the **PECB CISO certification exam**, an internationally recognized credential that validates your expertise and strengthens your credibility with both peers and employers (see the Certification tab for more information).

Objectifs

By the end of the PECB CISO training, you will be able to:

- Understand the key principles and essential concepts of information security
- Recognize the responsibilities of the Chief Information Security Officer (CISO), along with the ethical considerations and challenges of the role
- Create an information security program tailored to the specific needs of the organization
- Apply relevant frameworks, laws, and regulations, and implement effective security policies to ensure compliance
- Identify, analyze, assess, and treat information security risks in a structured and effective manner
- Prepare effectively for the PECB Certified Chief Information Security Officer (CISO) exam

Points forts

- **Learn from recognized experts**: our trainers are seasoned professionals in information security, with significant corporate experience and in-depth knowledge of the latest trends.

- **Apply your knowledge in practice**: immerse yourself in real-life scenarios through essay-type exercises, multiple-choice questions, and a comprehensive 450-page coursebook designed to prepare you for real-world challenges.
- **Validate your professional commitment**: earn 31 Continuing Professional Development (CPD) credits, demonstrating your investment in your career and your ongoing development.
- **Take the PECB CISO certification exam at no extra cost**: the internationally recognized PECB CISO certification is included in the training fee. In case of failure, you benefit from a free second attempt within 12 months.
- **Expand your professional network**: broaden your circle of contacts by exchanging with other participants and meeting information security experts, creating opportunities for collaboration and career growth.

Certification

*This training allows you to take the **PECB Chief Information Security Officer (CISO)** professional certification exam. A coupon code will be provided at the end of the course so that you can schedule your exam online.*

PECB CISO exam details:

The PECB Chief Information Security Officer exam is **available in French**. Format: multiple-choice exam with **80 questions**. Duration: **3 hours maximum**. The exam meets the requirements of the PECB Examination and Certification Program. It covers the following competency domains:

- Fundamental concepts of information security
- The role of the CISO in an information security program
- Selecting a security compliance program, including risk management, security architecture, and design
- Operational aspects of information security measures, incident management, and change management
- Promoting a culture of information security
- Monitoring and improving an information security program

After successfully passing your exam, you may apply for one of the certifications depending on your professional experience.

Qualifications	Exam	Professional Experience	ISMS Project Experience	Other Requirements
PECB Certified Information Security Officer	PECB Chief Information Security Officer Exam	None	None	Sign the PECB Code of Ethics
PECB Certified Chief Information Security Officer	PECB Chief Information Security Officer Exam	5 years, including 2 years of experience in information security management	Project activities totaling 300 hours	Sign the PECB Code of Ethics

For more details on the requirements, please refer to the PECB Examination Rules and the PECB Certification Rules .

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Attending this training requires the following prerequisite:

- Prior knowledge of the fundamental principles of information security, such as threats, vulnerabilities, and risks.

Public

This training is intended for information security professionals who want to strengthen their management and leadership skills, including:

- Information Security Managers (ISMs) / Chief Information Security Officers (CISOs)
- IT Managers
- Security Architects, Analysts, and Auditors
- Risk and Compliance Management Professionals
- Experienced CISOs
- Executives (CIOs, CEOs, or COOs)
- Any professional aspiring to leadership positions in information security

Programme

Day 1: Understanding the Fundamentals of Information Security and the Role of a CISO

- Introduction to information security (issues, challenges, and current trends)
- Fundamental principles of information security (Confidentiality, Integrity, and Availability – CIA)
- Identifying threats and vulnerabilities (risk assessment)
- The role of the CISO (responsibilities, skills, and essential qualities)
- Integrating ethics and professionalism into information security

Day 2: Building a Compliance Program, Managing Risks, and Designing Security Architecture

- Information security frameworks (ISO/IEC 27001, NIST, etc.)
- Laws and regulations related to information security (GDPR, etc.)
- Creating a compliance program (policies, procedures, and controls)
- Implementing risk management (identification, analysis, assessment, and treatment)
- Applying security architecture and design (principles and best practices)

Day 3: Implementing Security Measures, Managing Incidents, and Handling Change

- Selecting technical security measures (firewalls, antivirus, encryption, etc.)
- Defining organizational security measures (policies, procedures, training, etc.)
- Implementing physical security measures (access control, surveillance, etc.)
- Managing security incidents (detection, analysis, response, and recovery)
- Managing change (processes and best practices to minimize risks)

Day 4: Promoting Security Awareness, Ensuring Monitoring, and Supporting Continual Improvement

- Implementing information security awareness: importance and effective methods
- Monitoring and measuring security (Key Performance Indicators – KPIs)
- Encouraging continual improvement of security (identifying weaknesses and corrective actions)
- Developing leadership and communication in information security

Day 5 (half-day): Preparing for the PECB CISO Certification Exam

- Review of key topics covered throughout the training
- Detailed presentation of the exam (structure, format, and topics covered)
- Tips and strategies for exam success (methodology, time management, etc.)

Training content provided in partnership with PECB