CYBERSTRAT
Tailor-made advisory, solutions & training

PECB

PECB Chief Information Security Officer

Master the ability to establish and monitor an information security program

Why should you attend?

In recent years, there has been a growing recognition within organizations that they need a designated individual who has the necessary skills to effectively address information security responsibilities. Consequently, the role of the CISO has emerged as an executive-level position, obtaining the information security responsibilities that previously were held by personnel within the IT Department. Now, organizations have a dedicated professional focused on overseeing and managing all aspects of information security, ensuring a more comprehensive and specialized approach to safeguarding information and information assets.

By attending the PECB CISO training course, you will gain the necessary expertise to oversee and manage information security, ensuring the implementation of robust security measures, the identification and mitigation of information security risks, and the development of effective security strategies tailored to the organization's specific needs. In addition, by obtaining the PECB CISO credential, you demonstrate commitment to professional development and ability to take on executive-level responsibilities. Moreover, you will be able to enhance your career prospects, positioning yourself as a highly qualified candidate for senior leadership roles in the field of information security.

The PECB Chief Information Security Officer training course provides you with valuable insights and enables you to develop a comprehensive understanding of the role of a CISO and the steps involved in effectively managing information security within an organization. The training course covers a wide range of topics, including security frameworks, risk assessment, regulatory compliance, and governance. By attending this training course, you will gain knowledge of emerging security trends and best practices. Additionally, you will learn about the technologies that are essential to information security, including network security, application security, and cloud security.

Who should attend?

This training course is intended for:

- Professionals actively involved in information security management
- IT managers responsible for overseeing information security programs
- Security professionals who aspire to advance into leadership roles, such as security architects, security analysts, and security auditors
- Professionals responsible for managing information security risk and compliance within organizations
- Experienced CISOs seeking to enhance their knowledge, stay up to date with the latest trends, and refine their leadership skills
- Executives, including CIOs, CEOs, and COOs, who play a crucial role in decision-making processes related to information security
- Professionals aiming to achieve executive-level roles within the information security field

Course agenda

Duration: 5 days

Day 1 | Fundamentals of information security and the role of a CISO

- Training course objectives and structure
- Fundamentals of information security
- Chief information security officer (CISO)
- Information security program

Day 2 | Information security compliance program, risk management, and security architecture and design

- Information security compliance program
- Analysis of the existing information security capabilities
- Information security risk management
- Security architecture and design

Day 3 | Security controls, incident management, and change management

- Information security controls
- Information security incident management
- Change management

Day 4 | Information security awareness, monitoring and measurement, and continual improvement

- Awareness and training programs
- Monitoring and measurement
- Assurance program
- Continual improvement
- Closing of the training course

Day 5 | Certification Exam

Learning objectives

By the end of this training course, participants will be able to:

- Explain the fundamental principles and concepts of information security
- Comprehend the roles and responsibilities of the CISO and the ethical considerations involved, and address the challenges associated with the role
- Design and develop an effective information security program, tailored to the needs of the organization
- Adopt applicable frameworks, laws, and regulations and effectively communicate and implement policies to ensure information security compliance
- Identify, analyze, evaluate, and treat information security risks, using a systematic and effective approach

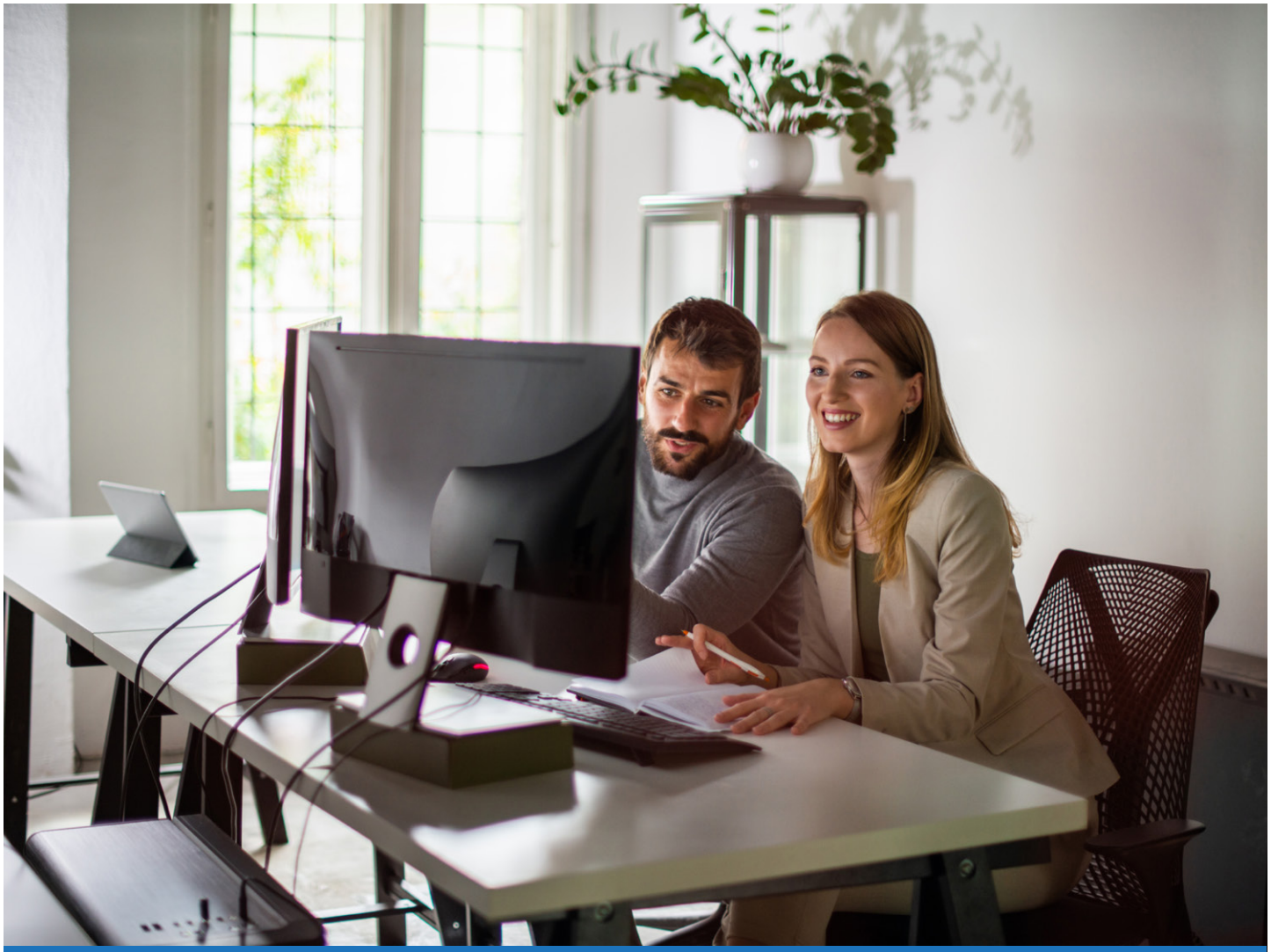
Examination

Duration: 3 hours

The "PECB Chief Information Security Officer exam meets the requirements of the PECB Examination and Certification Program (ECP). It covers the following competency domains:

Domain 1	**Fundamental concepts of information security**
Domain 2	**The role of CISO in an information security program**
Domain 3	**Selecting a security compliance program, risk management, and security architecture and design**
Domain 4	**Operational aspects of information security controls, incident management, and change management**
Domain 5	**Fostering an information security culture, monitoring, measuring, and improving an information security program**

For specific information about exam type, languages available, and other details, please visit the List of PECB Exams and the Examination Rules and Policies.



Certification

After successfully passing the exam, you can apply for one of the credentials shown below. You will receive the certificate once you comply with all the requirements related to the selected credential.

The requirements for PECB Chief Information Security Officer certifications are as follows:

Credential	Exam	Professional experience	InfoSec management experience	Other requirements
PECB Information Security Officer	PECB Chief Information Security Officer exam	None	None	Signing the PECB Code of Ethics
PECB Chief Information Security Officer	PECB Chief Information Security Officer exam	**Five years:** Two years of work experience in information security	Project activities: a total of 300 hours	Signing the PECB Code of Ethics

General information

- Certification and examination fees are included in the price of the training course
- Participants will be provided with the training course material containing over 450 pages of explanatory information, examples, best practices, exercises, and quizzes.
- An attestation of course completion worth 31 CPD (Continuing Professional Development) credits will be issued to the participants who have attended the training course.
- In case candidates fail the exam, they can retake it within 12 months following the initial attempt for free.