



CISO Certification

 Online instructor-led
Self-study
E-Learning
Modality

 English
Spanish
Language

 5 days
Duration






Gain the expertise to lead and govern information security programmes with the PECB Chief Information Security Officer course. In 5 days, you'll gain the strategic, technical, and operational skills to build and oversee a comprehensive information security programme aligned with frameworks, laws, and industry standards.

Designed for professionals advancing into executive roles, this course covers everything from risk management and compliance to architecture design, awareness programmes, and incident response. Upon passing the exam, you can apply for the PECB Chief Information Security Officer credential — a globally recognised validation of your ability to lead and manage enterprise-level information security.

Learning Objectives

By the end of the course, you will be able to:

-  Comprehend core information security concepts
-  Understand the CISO's responsibilities, ethical duties, and address the main challenges of the role.
-  Design and lead an information security programme tailored to organisational needs

- ✓ Integrate frameworks, laws, and compliance requirements into governance processes
- ✓ Identify, analyze, evaluate, and treat information information security risks using a systematic, actionable approach
- ✓ Oversee operational aspects such as incident response, change management, and continuous improvement

• Who Should Attend?

- 🔍 Professionals actively involved in information security management
- 👤 IT managers overseeing security programmes
- 🛡️ Security professionals who aspire to advance into leadership roles, such as security architects, security analysts, and security auditors
- 📁 Compliance and risk managers involved in InfoSec strategy
- 💻 Current CISOs seeking to enhance their knowledge, stay up to date with the latest trends, and refine their leadership skills
- 🏢 C-level executives (CIOs, CEOs, COOs) involved in security decision-making

• What's Included?

- 📁 450+ pages of course material, exercises, case studies, and examples
- 📄 Certification and exam fees
- 🏆 Course completion attestation, granting 31 CPD credits.

• Course Agenda

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.

Certification & Exam

Certification Prerequisites


After passing the exam, you can apply for one of the credentials listed in the table below. You will receive a certification once you fulfill all the requirements of the selected credential.

	PECB Information Security Officer	PECB Chief Information Security Officer	Other requirements
General Work Experience	None	5 Years	
Information security experience	None	2 years	Signing the PECB Code of Ethics
Information Security management experience	None	300 hours	

 **Exam:** 3 hours, taken on Day 5

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.

 **Maintenance Fee:** First year included; fees applies from second year. Pay \$120/year or save 10% by paying three years upfront.

