Data Protection
institute

# CISO Training Track

## The foundations of your CISO skills development

### Become a certified CISO in 7 modules

*Join us today and take the first step towards becoming a top-notch Certified CISO!*

# Modules

# Introduction

Thank you for your interest in our training trajectory to become a certified Chief Information Security Officer (CISO).

As the world becomes increasingly digitized, the complexity of cyber security continues to rise. This has resulted in a growing need for highly trained professionals who can navigate the challenges and risks associated with the protection of sensitive information. The role of the CISO has become more important than ever before.

As a CISO, you would be responsible for a multitude of tasks, including developing and implementing security strategies, monitoring compliance with security policies and regulations, and overseeing incident response and recovery efforts. In addition, you would be tasked with bridging the gap between the information security staff and the management/board. This requires excellent communication skills and the ability to translate technical information into business language.

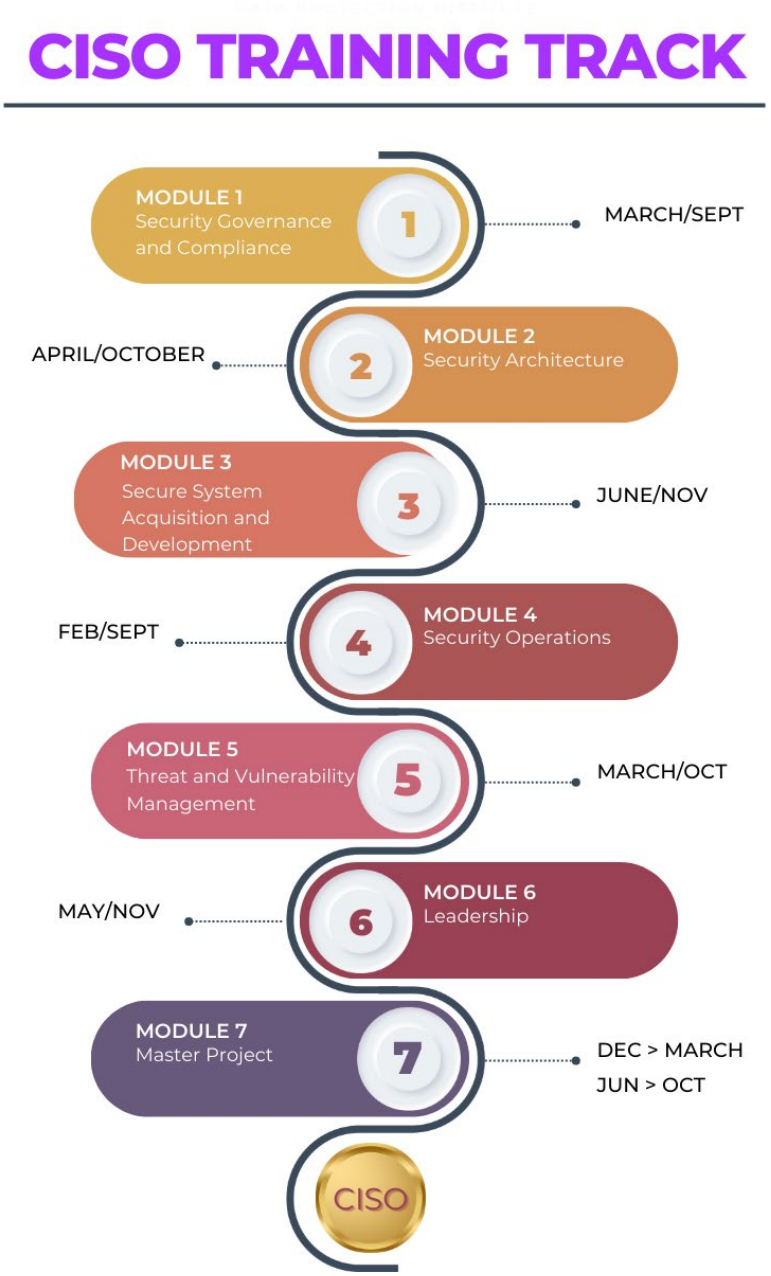
At our institute, we offer a comprehensive course trajectory designed specifically to prepare Information Security Officers - or anyone wishing to perform a coordinating role in the field of information security - for the demands of the role that the Chief Information Security Officer plays, either as part of an organization's workforce, or as an independent freelance CISO.

The separate modules of this CISO course trajectory cover a wide range of topics, from risk management and compliance to incident response and communication skills. Our experienced instructors provide hands-on training, using real-world scenarios to help you develop the skills and knowledge you need to succeed.

By completing our CISO course and obtaining your certification as a CISO, you will be well-equipped to take on the challenges of this critical role and help your organization stay secure in the face of ever-evolving cyber threats.

# Overview

The modules of the CISO track can be started in the Spring or in the Autumn. Although there is a calculated order in the sequence of the modules, each module (from 1 to 6) can stand on its own and they can be taken up in a random order, in case a course participant is unable to take up a particular module. In that case, they can choose to take up the module later in the year or the following “semester”. Module 7 consists of a master project (infra) that can only be started when modules 1 to 6 have been completed. We foresee a total period of 18 to 24 months to finish all the modules from 1 to 7. You will find more information on each of the modules on the following pages.



# 1 Security Governance and Compliance

Get ready to kickstart your journey towards becoming a Certified CISO with our module 1. In this module, we'll cover the basics and highlight **the crucial difference between information security and cybersecurity**.

We'll guide you through the process of defining, implementing, and managing an Information Security Governance Programme. You'll learn how to organize security, the responsibilities of personnel involved, and get an overview of laws, regulations, and standards that affect your security governance programme.

Critical questions such as how to establish policies, processes, and standards and how to turn them into an **actionable security strategy** aligned with your company's objectives, will be answered here. The importance of a security awareness programme will get great emphasis and we will show you how it can reduce corporate risk.

Additionally, we'll provide you with the tools and facts you need to develop a **robust security culture** that is inherently appealing.

Finally, we'll help you navigate internal and external audits, including putting your **audit programme** in place and complying with external audits.

**Quick learning & development checklist:**

- ★ The basics of creating and running a Security Governance Programme.
- ★ How to operationalise this programme with the appropriate expertise and effectively boost your company’s security stance.
- ★ How to measure and improve your programme, based on regular risk assessments and audits.
- ★ How to demonstrate the imperative worth of a Security Governance Programme to management.
- ★ Why conducting regular security awareness initiatives is crucial and how to put them together.

# 2 Security Architecture

The second module of the Certified CISO training programme focuses on **security architectures**, covering both theoretical architecture models and practical implementations. The course includes discussions on IoT, OT/ICS, and cloud security concepts, as well as business continuity and disaster recovery planning.

While the technical nature of the content may seem daunting, the module is designed to provide you with just enough knowledge to have informed conversations with your security architects. As a CISO, it's important **to bridge the gap between business risks and technical security strategies**, and this course is tailored towards achieving that goal.

By the end of the module, you will have a strong understanding of commonly used architectural frameworks, how security fits within them, and how to effectively manage these components. Alongside the theoretical content, the module also provides practical advice and pointers on key areas such as IoT security, OT/ICS security, cloud security, and business continuity/disaster recovery.

This module will equip you with a solid foundation in security architectural setups and practices, applicable across a range of sectors.

**Quick learning & development checklist:**

- ★ The meaning behind so-called “zero trust” architectures.
- ★ The major enterprise architecture frameworks and how security fits in.
- ★ The various cloud service models and the various security features associates with them.
- ★ The “shared responsibility” model when using cloud services and possible pitfalls and areas of attention.
- ★ OT/ICS security and how it differs from IT security.
- ★ Internet of Things major risks and current initiatives to tackle the issues.
- ★ Disaster Recovery and Business Continuity: what’s the difference, how to create a BCP and how to apply high-availability principles in our architecture?

# 3 Secure System Acquisition and Development

Our module 3 on Secure System Acquisition and Development, will teach you how to approach software security from the governance, compliance, and risk perspectives, as the main software security stakeholder.

We'll guide you through the process of building security and privacy into your organization's software acquisition, development, and management practices, considering various factors such as company structure, stakeholder priorities, and existing technical debt. Discover how to **integrate security** into waterfall, agile, and DevOps ways of working and explore frameworks that can help you achieve this.

When it comes to evaluating, purchasing, or developing systems and applications, or using cloud services, you'll learn how to ensure that the correct and relevant **security requirements** are documented and checked before making any decisions.

CI/CD (Continuous Integration / Delivery) **pipelines** are the way to go for modern, cloud-based infrastructures. You'll learn what they are, why they're important, and the security advantages of automation.

Finally, discover **how to implement security requirements and test them effectively** using techniques such as SAST, DAST, and IAST. We'll teach you how to set up and improve a Secure Software Program (SSP) to manage the identification, analysis, and specification of information security requirements, securing application services in development and support processes, and more.

This module will equip you with the skills and knowledge needed to ensure the security and privacy of your organization's software, as the core action of the CISO's function.

**Quick learning & development checklist:**

- ★ The Software Security Program
- ★ Security / Privacy by design & by default
- ★ Setting security requirements
- ★ Securing CI/CD pipelines & automation
- ★ Security Testing

# 4 Security Operations

This training module is designed to teach CISOs **how to effectively combine information security and IT operations practices** to improve collaboration and reduce risks. The following topics will be covered:

- **Asset Management**: You will learn how to identify and manage your most important assets, including data and physical assets like devices and applications. We'll cover BYOD, BYOK, CYOD, and vendor support to ensure assets are secure and still supported.

- **Identity and Access Management:** Controlling user access to resources is a challenging activity. We will teach you about modern cloud and non-cloud authentication techniques, identity governance and administration platforms, PKI, and privileged identity and access management, as well as encryption and key management.

- **Network Security**: Our trainers will teach you how to secure access to wired, wireless, and cloud networks. We will also cover physical security components, such as badge readers, camera systems, and burglary alarms.

- **Outsourcing Security Operations**: Certain aspects of security operations can be expensive and may be a candidate for outsourcing. We will discuss the most common security operations to outsource and which aspects deserve your attention. Additionally, we will cover the KPIs and SLAs that should be put in place.

At the end of this training, you will have a solid understanding of how to practically set up and improve your organization's security operations, as well as how to effectively manage your most important assets, user access, and network security. This training is essential for any CISO looking to run and improve their organization's security operations.

**Quick learning & development checklist:**

★ Get control over your most important assets.
★ Better manage your organization identities and access.
★ Understand how to protect your organization devices.
★ Apply best practices to physical security.
★ Outsource your security operations without losing control.

# 5 Threat & Vulnerability Management

Module 5 is designed to provide CISOs with a comprehensive understanding of threat and vulnerability management as part of the security programme. Throughout the course, you will learn how to set up, manage, and measure the threat and vulnerability process.

The module will begin by covering the identification and logging of security events, including the use of SIEM (Security Incident and Event Management) tools to capture and correlate logs. You will also learn about SOC (Security Operating Center) and how it is used to monitor all events and correlations.

Next, the instructors will delve into different frameworks such as MITRE Att&ck, which reflects various phases of an attack lifecycle and documents attacker tactics and techniques based on real-world observations. You will also learn about different types of hacking, including whiteboard hacking (aka Threat Modelling), and Penetration Testing by ethical hackers.

The course will cover various kinds of penetration tests, such as blue, red, and purple teams, and will also discuss the insider threat as employees can sometimes be the first "hackers" you will be confronted with.

Finally, the course will conclude with a focus on vulnerability and patch management, as a well-defined and properly managed management of vulnerabilities is crucial for preventing threats and increasing security resilience.

**Quick learning & development checklist:**

- ★ Learn your role as a CISO in threat and vulnerability management.
- ★ Understand the concepts of SIEM and SOC to monitor threats.
- ★ Know the role of hacking in your security program.
- ★ Be successful in the management of vulnerabilities and patches.

# 6 Leadership

Being a CISO goes beyond understanding threats, technology or infosec policies. It's equally, if not more important to explain the why and how to your senior management, your executives, or your Board. And did you already wonder how will you address the skills shortage on today's labour market?

We will guide you through the process of identifying your stakeholders, but also give you some practical tips in communicating your (cyber)security strategy and budget needs.

Some of the critical questions we cover include issues like:

Who are your stakeholders being a CISO?
How can you communicate effectively with your Board and senior management?
How to attract, train and keep your CISO staff?

**Quick learning & development checklist:**

- ★ The position of a CISO in the organization.
- ★ How to demonstrate your value as CISO to your stakeholders.
- ★ How to influence your organization.
- ★ Measure what matters, and tell a story.
- ★ Do's and Don'ts of presenting cyber to your Board.
- ★ Attract, train, and retain information security talent.

# 7 Master project

After finishing modules 1 to 6, completing a self-assessment questionnaire and participating in an orientation session which will result in a "case selection guidance report", you will be able to start working on your master project with an attributed mentor.

The focus of the selection will be on one or more of the items that were covered in modules 1 to 6:

- Security Governance and compliance (example: impact of NIS2 on the security program)
- Security architecture (example: migration to cloud based on zero trust concepts)
- Secure system acquisition and development (example: definition of secure testing requirements)
- Security operations (example: defining privileged identity program)
- Threat and Vulnerability management (example: how to integrate a SOC into the security program)
- Leadership (example: stakeholder management)

The master project is a written document that contains:

- The Case selection guidance report;
- The problem statement as well as the working methodology & approach;
- Documentation (including evaluations) of the feedback sessions of the promotor;
- The master project (DPI template) that contains a management report;
- Handouts of a board presentation, that is the presentation as discussed in step 7 of the certification process.

According to the evaluation criteria for the master project – which are based on the CISO competence profile as defined by ENISA in their European cybersecurity skills framework – a jury will evaluate your master project and decide if you pass or fail for this master project.

The overall goal of the master project is for you to to acquire the CISO Certificate of Completion. The certification will not follow the ISO 170241 process (certification of persons), but we will respect the steps where relevant and feasible.

## Dates 2023 – 2024

| | | |
|---|---|---|
| 24-25/04/2023 | CISO 2: Security Architecture | Diegem |
| 08-09/05/2023 | CISO 6: Leadership | Diegem |
| 12-13/06/2023 | CISO 3: Secure System Acquisition and Development | Diegem |
| June 2023 | CISO 7: start master projects | |
| | | |
| 20-21/09/2023 | CISO 1: Security Governance and Compliance | Antwerp |
| 26-27/09/2023 | CISO 4: Security Operations | Diegem |
| 17-18/10/2023 | CISO 2: Security Architecture | Mechelen |
| 24-25/10/2023 | CISO 5: Threat and Vulnerability Management | Mechelen |
| 21-22/11/2023 | CISO 3: Secure System Acquisition and Development | Mechelen |
| 29-30/11/2023 | CISO 6: Leadership | Mechelen |
| December 2023 | CISO 7: start master projects | |
| | | |
| 08-09/02/2024 | CISO 4: Security Operations | Diegem |
| 19-20/02/2024 | CISO 1: Security Governance and Compliance | Diegem |
| 21-22/03/2024 | CISO 5: Threat and Vulnerability Management | Diegem |
| 22-23/04/2024 | CISO 2: Security Architecture | Diegem |
| 13-14/05/2024 | CISO 6: Leadership | Diegem |
| 10-11/06/2024 | CISO 3: Secure System Acquisition and Development | Diegem |
| June 2024 | CISO 7: start master projects | |
| | | |
| 19-20/09/2024 | CISO 1: Security Governance and Compliance | Antwerp |
| 25-26/09/2024 | CISO 4: Security Operations | Antwerp |
| 15-16/10/2024 | CISO 2: Security Architecture | Antwerp |
| 23-24/10/2024 | CISO 5: Threat and Vulnerability Management | Antwerp |
| 25-26/11/2024 | CISO 3: Secure System Acquisition and Development | Antwerp |
| 04-05/12/2024 | CISO 6: Leadership | Antwerp |
| December 2024 | CISO 7: start master projects | |

## Pricing

Per module (1 to 6, excluding 7) : **EUR 1.395 excl. VAT**
Entire track (7 modules) : **EUR 8.695 excl. VAT**

KMO-portefeuille (Flanders) offers a higher educational fee for cybersecurity courses: 45% for small and 35% for medium-sized companies. Check the website for more information: https://www.vlaio.be/nl/subsidies-financiering/kmo-portefeuille.