Cyber Information Security Leader

An education enabling cybersecurity leaders and specialists in navigating the corporate landscape

Education Program 2024

Contact info

Katharina Bengtsen (Coordinator)
Phone: + 45 53 54 88 67
Mail: kb@cisl.dk

ISACA Denmark Chapter

Kopenhagen Konsulting

KRAGERUP GODS

CISL CYBER INFORMATION SECURITY LEADER

Introduction

Cyber Information Security Leader (CISL) is an education designed to train cybersecurity managers and specialists, enabling them to safely lead organizations through the challenges of digitalization.

Despite the high priority of cybersecurity among top management, many professionals still encounter significant barriers when it comes to cybersecurity management. Usually recruited from specialist roles, they often refer to a couple of common shortcomings: business language and logic, and corporate governance.

As organizations grow, building and developing teams of extremely focused and different specialists are increasingly becoming central to their responsibility. This can be an overwhelming challenge. Therefore, this has a prominent position among other subjects in the CISL program.

The CISL education focuses on strengthening participants' capability to navigate at the executive level, managing politics, stakeholders, culture, and the corporate reporting game.

With an emphasis on personal leadership and the importance of people management in a competitive market for talent, participants are equally prepared to build and nurture diverse teams, coming from odd corners of the IT universe and neighbouring skills areas.

After the program, participants will have gained the insight and ability to handle the complex challenges surrounding their role.

The CISL Program

Approach

The CISL education employs a combination of lectures, real-life cases, and -exercises provided by instructors and guest lecturers, to facilitate open discussions. Participants will be assigned to groups and are expected to actively engage in various exercises. It is expected that participants allocate time for group work between modules as part of their preparation.

Prior to program start

Participants will complete a personality test and feedback session prior to the program start to assess their personality type and leadership profile. Two coaching sessions will follow up on individual development during the program.

Program & Modules

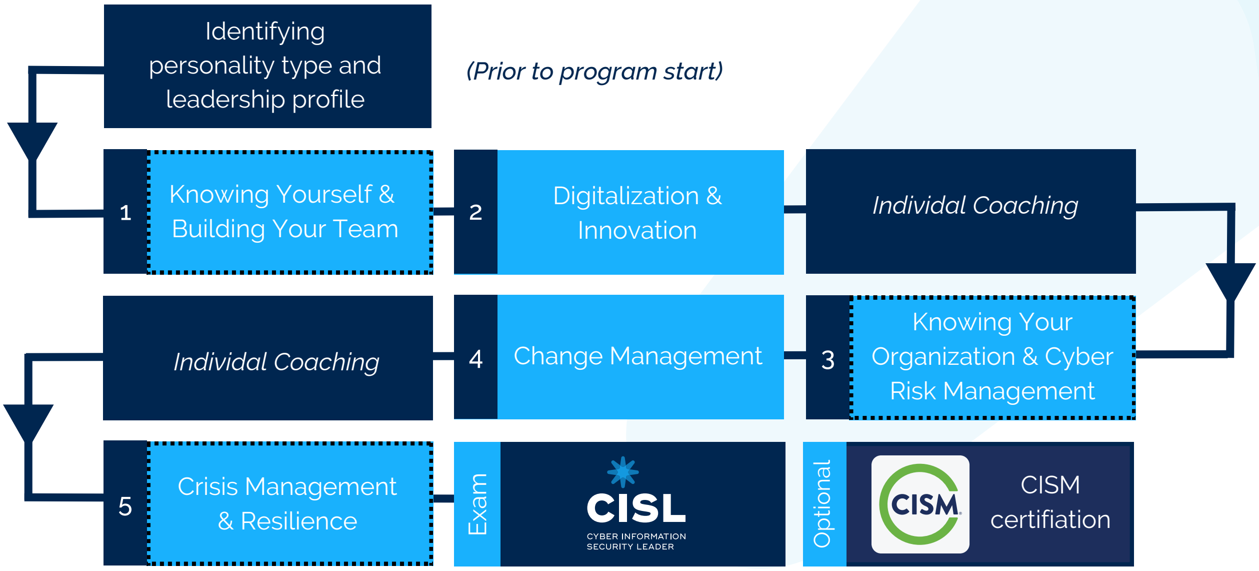
The program consists of five themed modules, divided into eight full-course days, and one exam date. Modules are scheduled from 08:30 - 17:30 except residential courses.

Modules 1, 3, and 5 (highlighted) are residential courses consisting of two full-course days. To pass the education and qualify for the exam, participants must attend at least 4 out of 5 modules. Throughout the program, each participant will develop an individual business case on a chosen subject. This is to be presented to a fictive 'Board of Directors' for the final exam.

CISM Certification (Optional)

Upon passing the final exam, CISL offers a CISM certification via ISACA Denmark Chapter. To sign up, please inform CISL coordinator at **kb@cisl.dk** when registering for CISL.

Fig. CISL Program Overview



Identifying personality type and leadership profile
(Prior to program start)
1
Knowing Yourself & Building Your Team
2
Digitalization & Innovation
Individal Coaching
3
Knowing Your Organization & Cyber Risk Management
4
Change Management
Individal Coaching
5
Crisis Management & Resilience
Exam
CISL
CYBER INFORMATION SECURITY LEADER
Optional
CISM
CISM certifiation

Learning Objectives

The five modules

The following outlines the knowledge, skills, and competencies that guide the training for each of the five modules.

Module 1: Knowing Yourself & Building Your Team

Knowledge	Skills	Competencies
Familiarity with personality types Recognize your strengths and challenges Understand the crucial match between cybersecurity strategies and the required skills in a diverse team of dedicated specialists	Identifying personality types of senior executives and other stakeholders Understand classical conflict patterns Recognize the natural diversity among team members and stakeholders - ensuring appropriate involvement in various situations and tasks	Improved convincing skills towards management Ability to strengthen relationships with important stakeholders Work effortlessly with people and stakeholder management Nurture the taste for individual growth while rewarding team efforts and achievements

Module 2: Digitalization & Innovation

Knowledge	Skills	Competencies
Recognize how innovation and digitalization maps into cybersecurity thinking, planning and behavior	Educate innovation teams on cybersecurity risks and provide a range of solution options	Proactively incorporate cybersecurity thinking into innovation planning Empower the business to generate and retain revenue during technology shifts and beyond

Module 3: Knowing Your Organization & Cyber Risk Management

Knowledge	Skills	Competencies
A realistic and recognizable overview of key roles, responsibilities and policies Understand underlying key business drivers Understand how the complex threat and risk picture, covering the entire value chain affects the organization Familiar with terms and processes appearing in the development and implementation of business ambitions	Engage relevant decision-makers when escalating cyber risk issues and requests Develop a business case based on relevant business drivers Elevate the significance of cyber risk Holistic mitigation of risk linked to the human factor Quantifying risk and consequences	Design appropriate escalation paths for risk events and mitigation investments Build business cases recognizable among decision-makers Effective communicate threats and the risk landscape, design appropriate risk mitigations, and secure comprehension and funding from senior executives Identify areas for improvement and create a recognizable narrative for the organization

Module 4: Change Management

Knowledge	Skills	Competencies
Understand the mechanisms driving change and implementation across the organization - in terms of inherited thinking, planning and behaviors	Ensure that cybersecurity is embedded in all stages of business planning and execution	Keeping focus on the human factor when implementing changes, both in individual perception and behavior, and in the total value chain

Module 5: Crisis Management & Resilience

Knowledge	Skills	Competencies
Strategies and best practices for navigating a crisis - before, during and after a crisis strikes Effective response procedures and crisis communication (Self) awareness and feedback on your behavioral patterns in a crisis	Ensure management buy-in for resilience building Develop and implement a crisis response plan for your organisation Mature management and stakeholders for crisis handling	Efficient communication with key stakeholders during a crisis Define ownership and design appropriate procedures and escalation paths Maintain overview and composure during a serious incident

> The strength of this education is the great opportunity to spare with industry peers and board members from different organizations. Understanding how board directors think and what they expect in terms of reporting, has been really valuable and applicable. I highly recommend CISL for any cybersecurity professional, who wants to aspire to leadership as it trains and prepares you for what you meet out there in real life

- Morten Dichmann Hansen, CISO, Copenhagen Airports A/S

> This is not a course that focuses on the technical aspects of cybersecurity – but this is also where I feel comfortable with my knowledge. This is a hands-on approach to leadership presented by industry-experienced instructors, who know what they are talking about – and that has been very inspiring

- Lars Gottschalk, Head of Analysts, TDC

Practical Information

Prior to program start

Upon registration, participants are required to sign an NDA to ensure confidentiality and mutual trust in discussions.

Dates for CISL Fall 2024

September 17 – 18th (Module 1)
October 1st & 22-23rd (Module 2, Module 3)
November 5th & 19-20th (Module 4, Module 5)
December 3rd: (Exam)

Location

Residential courses are held in the beautiful surroundings and facilities at Kragerup Gods located on west side of Zealand. Single modules are held at Matrikel1 located in central Copenhagen.

Price & Registration

Price 56.000 DKK ex. VAT for CISL only.
Price 68.000 DKK ex. VAT. including CISM.
Accommodation, catering & materials included.
To register for CISL click **here** or send mail to: **cts@cisl.dk** providing name, email, phone, and invoice information (company, attention, address, CVR, PO). The full price will be invoiced upon registration,

Cancellation or Changes

In case of cancellation less than 30 days before the first module, no refunds apply. It is possible to substitute a registered participant if the person is unable to attend, upon good notice. Cancellation requests will **only** be accepted in written form.

Contact information

Camilla Treshow Schrøder, CISL Co-Founder
cts@cisl.dk / + 45 41 27 12 57

Kragerup Gods,
Kragerupgårdsvej 33, 4291 Ruds-Vedby

CISL Alumni

Upon completing the course, participants will be invited to become a member of the CISL Alumni. A network dedicated to practicing and further developing the leadership disciplines introduced at CISL.

CISL Alumni is exclusively for certified CISL members, providing a strong network of cybersecurity leaders with diverse backgrounds and experiences.

The alumni facilitates an open and informal atmosphere, offering a confidential space, where members gather to discuss current topics and challenges related to their daily work within the field of cyber leadership. Members participate for inspiration, peer support, and networking.

> The strength of the program is definitely its strong network of speakers and real world board members, who make the topics both practical and relevant – but also its ability to create a unique forum for professional sparring and knowledge sharing among the various students and their individual organizations
>
> **- Michael Svendsen, CISO, NKT**

Membership information

2 stayover meetings per year
Yearly membership fee: 14.000 DKK ex. VAT.
Includes accommodation and catering.

CISL
CYBER INFORMATION SECURITY LEADER

Behind the Scene

About the initiators

The Cyber Information Security Leader (CISL) education was established in 2021 as a strong partnership between Camilla Treschow Schrøder, Klaus Kongsted, and Per Erik Sørensen.

Camilla is the founder of the cybersecurity talent supply organization Treschow&Son and a public speaker on leadership trends in cybersecurity. Klaus is co-founder of Dubex and one of Denmark's leading information security experts. Per Erik Sørensen is an experienced senior executive and board member.

A Kopenhagen Konsulting Partnership

Kopenhagen Konsulting is a management consulting company, offering strong expertise in cybersecurity management to the CISL program:

"We specialize in helping leaders navigate uncertain challenges and achieve strategic objectives through expertise in Cybersecurity and Digitalization. With an approach encompassing cascading strategy, project execution, and organizational management, we ensure that leaders are guided in making the right decisions and that mountains are moved when they need to be".

Special Contributors

Jakob Skytte, Partner, Kopenhagen Konsulting
Lasse Bolander, Vice Chairman, Coop Denmark
Jesper Lok, Board of Directors
Ken Bonefeld, CISO, Norlys
Shehzad Ahmad, Group CISO, Topdanmark
Jan Topp Rasmussen, CIO, Semco Maritime A/S
Patrick Miller, CEO, Ampere Industrial Security & SANS instructor
Peter Frøkjær, President, ISACA Denmark Chapter

Kopenhagen Konsulting

ISACA® Denmark Chapter

KRAGERUP GODS

CISL
CYBER INFORMATION SECURITY LEADER