CISL
CYBER INFORMATION SECURITY LEADER

Cyber Information Security Leader

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

Education Program 2024

Contact info
Camilla Treschow Schrøder
Phone: + 45 41 27 12 57
Mail: cts@cisl.dk

ISACA Denmark Chapter
Kopenhagen Konsulting
KRAGERUP GODS
CISL CYBER INFORMATION SECURITY LEADER

Introduction

Cyber Information Security Leader (CISL) is an educational program 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 managing cybersecurity. Often recruited from specialist roles, they commonly face two main shortcomings: understanding business language and logic, and corporate governance.

As cybersecurity becomes increasingly decentralized and relevant to multiple organizational business functions, the ability to drive change and facilitate collaboration, communication, and commitment is becoming central to their responsibilities. This can be an overwhelming challenge. Therefore, these skills hold a prominent position among other subjects in the CISL program.

The CISL program focuses on strengthening participants' capabilities to navigate at the executive level, managing politics, risks, stakeholders, crises, culture, and corporate reporting.

With an emphasis on personal leadership, participants are also introduced to the value of understanding how personality types, their capabilities, and their behavioral structures can be strategically used to create impact and drive results, especially in crisis situations.

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

The CISL Program

Approach

The CISL program 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. Additionally, participants are expected to allocate time for group work between modules as part of their preparation.

Prior to the Program Start

Participants will complete an initial coaching session to define individual learning objectives and development areas. Two additional coaching sessions will follow up on individual development during the program.

Program & Modules

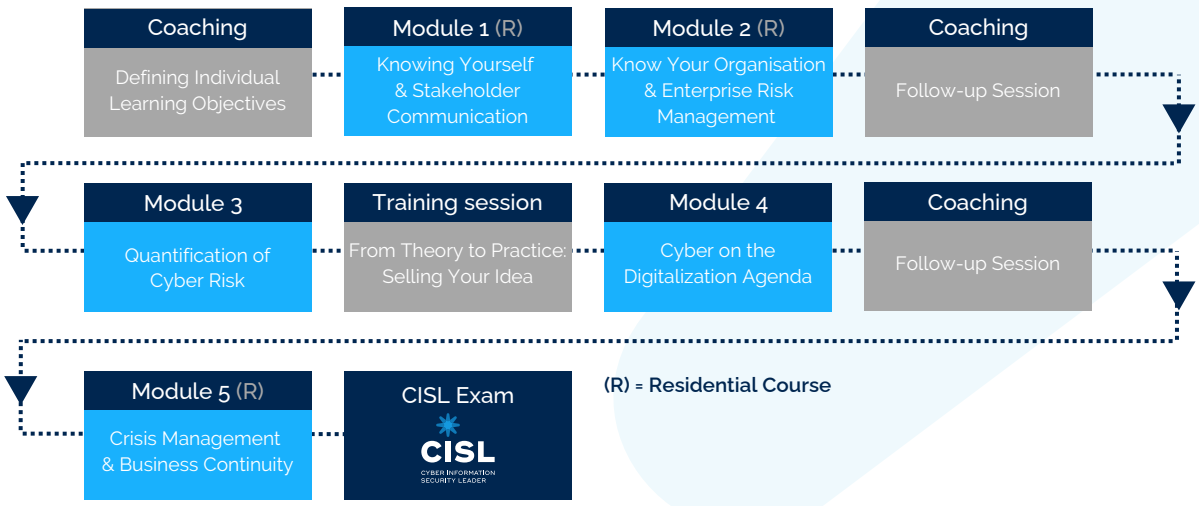
The program comprises five themed modules, divided into nine full-course days and an exam date. Days are scheduled from 08:30 to 17:30, except for residential courses (modules 1, 3, and 5), which consist of two full-course days each.

To pass the program and qualify for the exam, participants must attend at least four out of the five modules. Throughout the program, each participant will develop an individual business case on a chosen subject, to be presented to a fictitious 'Board of Directors' for the final exam.

CISM Certification (Optional)

After passing the final exam, CISL offers optional CISM certification through ISACA Denmark Chapter. To sign up, please inform Camilla Treschow at cts@cisl.dk or check the box when signing up **online**.

Fig. CISL Program Overview



Learning Objectives

The five modules

The following outlines the knowledge, skills, and competencies that are covered in each of the five modules.

Module 1: Knowing Yourself & Stakeholder Communication

Knowledge	Skills	Competencies
Familiarity with the Enneagram and its personality types Recognize your personal strengths and challenges and how they project in your leadership Understand how to use your personal strenghts and characteristics to create impact	Identifying personality types of senior executives and other stakeholders Understand classical conflict patterns Recognize the natural diversity among 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

Module 2: Know Your Organisation & Enterprise Risk Management

Knowledge	Skills	Competencies
A realistic and recognizable overview of key roles, responsibilities and policies in the organization Understand underlying key business drivers Understand the mechanisms driving change and implementation across the organization - in terms of inherited thinking, planning and behaviors	Engage relevant decision-makers when escalating cyber risk issues and requests Develop a business case based on relevant business drivers Ensure that cybersecurity is embedded in all stages of business planning and execution	Design appropriate escalation paths for risk events and mitigation investments Build business cases recognizable among decision-makers Keeping focus on the human factor when implementing changes, both in individual perception and behavior, and in the total value chain

CISL
CYBER INFORMATION SECURITY LEADER

Module 3: Quantification of Cyber Risk

Knowledge	Skills	Competencies
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	Elevate the significance of cyber risk Holistic mitigation of risk linked to the human factor Quantifying risk and consequences	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: Cyber on the Digitalization Agenda

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 5: Crisis Management & Business Continuity

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

CISL
CYBER INFORMATION SECURITY LEADER

IThe strength of this program lies in the great opportunity to interact with industry peers and board members from various organizations.
Understanding how board directors think and what they expect in terms of reporting has been incredibly valuable and applicable.
I highly recommend CISL for any cybersecurity professional aspiring to leadership, as it trains and prepares you for real-life challenges.

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

This course does not focus on the technical aspects of cybersecurity, which I already feel comfortable with. Instead, it offers a hands-on approach to leadership presented by industry-experienced instructors who truly understand their subject matter — 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

Module 1
4. - 5. Sept.

Module 2
16. - 17. Sept.

Module 3
1. Oct.

Training sess.
24. Oct.

Module 4
5. Nov.

Module 5
19. - 20. Nov.

Exam
3. Dec.

Location

Residential modules 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.

Contact information

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

Price & Registration

Price 68.000 DKK ex. VAT for CISL only.
Price 78.000 DKK ex. VAT. including CISM
Accommodation, catering, and materials are included. CISM exam fee is excluded from the price.

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.

Kragerup Gods,
Kragerupgårdsvej 33, 4291 Ruds-Vedby

CISL
CYBER INFORMATION SECURITY LEADER

CISL Alumni

Upon completing the course, participants will be invited to join 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 in cyber leadership. Members participate for inspiration, peer support, and networking.

> The strength of the program lies in its strong network of speakers and real-world board members, who ensure the topics are practical and relevant. Additionally, it creates a unique forum for professional sparring and knowledge sharing among the students and their respective organizations.
>
> **- Michael Svendsen, CISO, NKT**

Membership information

2 stayover meetings per year and a 1 day company visit.
Yearly membership fee: 12.000 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 through a strong partnership involving 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 the 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 that offers 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".

Kopenhagen Konsulting

ISACA Denmark Chapter

KRAGERUP GODS

Special Contributors

Jakob Skytte, Partner, Kopenhagen Konsulting.
Daniel Shepherd, CEO, CSIS Security Group A/S.
Jesper Lok, Board of Directors.
Ken Bonefeld, CISO, Norlys.
Shehzad Ahmad, Group CISO, Topdanmark.
Jonas Roos Christiansen, IT Respond & Revovery Manager, Copenhagen Airports A/S.
Peter Frøkjær, President, ISACA Denmark Chapter.
Hanne Hansen, tidl. CISO, Energinet.
Jens Rasmussen, tidl. CIO, Chr. Hansen A/S / Novonesis.
Martin Stausbøll, CISO, COWI.

CISL
CYBER INFORMATION SECURITY LEADER