

# Cyber Information Security Leader

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

**Education Program 2027**

# 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 the new corporate landscape managing business strategy, politics, risks, stakeholders, crises, culture, and executive 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.

# About the Program

## Approach

The CISL program employs a combination of lectures, guest speakers, real-life cases, and exercises provided by instructors 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

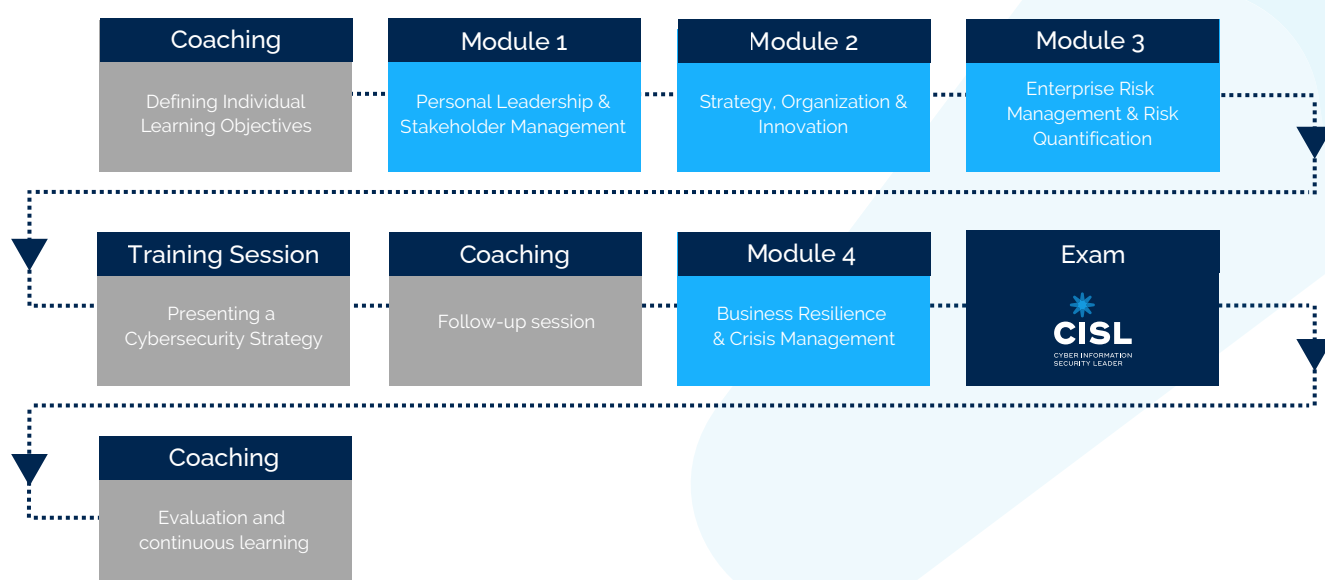
The program comprises of 9 full-course days. Course days are divided into 4 themed modules and a training session. Module 1, 3 and 4 constitute residential courses to promote a strong network and to foster ongoing dialogue among participants.

The program ends with a final individual exam, where participants will present a business case to a fictitious 'Board of Directors'. To pass the program and qualify for the exam, participants must attend at least 8 out of the 9 course days.

## CISM Training (Optional)

In addition to CISL, participants can attend a 4-day CISM exam training course preparing for a CISM certification through ISACA Denmark. For price information see: **Practical Information**.

Fig. CISL Program Overview



# Modules & Learning Objectives

## Module 1: Personal Leadership & Stakeholder Management

This module introduces key concepts and frameworks to guide effective communication with teams and organizational stakeholders - foundational elements of the CISL program. The module presents the Enneagram as a framework for understanding individual leadership capabilities, challenges, and different communication styles to manage relationships and conflicts more effectively. As stakeholder management is key to success in change management, the module explores essential aspects of stakeholder communication, equipping participants with strategies to build trust and practical techniques for engaging, convincing, and influencing key stakeholders.

**Keywords:** Foundational Frameworks, Personal Leadership, The Enneagram, Stakeholder Management, Stakeholder Communication, and Change Management.

**Outcome:** Participants will gain the skills to tailor communication strategies that resonate with stakeholders, enabling them to craft a compelling and recognizable narrative, appeal to relevant business drivers, and build trust to drive greater engagement, support, and impact.

## Module 2: Part 1: Strategy & Organization

This module explores the business strategy and organizational landscape of executive stakeholders. With insights into the mindset, roles, priorities, and decision-making processes of executives, the module illustrates ways to improve communication and frame the cybersecurity agenda in a way that resonates with top management—securing alignment, commitment, and buy-in for cybersecurity initiatives. The module will also cover key principles for designing a cybersecurity function that fits the organization. Addressing questions of references, headcounts, governance, and design, participants will get inspiration for how to build a cybersecurity organization that not only supports the business but serves as a strategic enabler of resilience.

**Keywords:** Business Strategy, Executive Mindset, Executive Communication, Board of Directors, Cybersecurity Reporting, Governance Structures, and Cybersecurity Organization and Design.

**Outcome:** Participants will get perspectives on how to strengthen collaboration and communication with executive stakeholders with greater impact.. align cybersecurity efforts—including organizational design and governance structures—with broader business priorities.

# Modules & Learning Objectives

## Module 2: Part 2: Strategy & Innovation

This module deepens the exploration of the organizational landscape with a focus on understanding organizational mechanisms and the intersection between business strategy, digital strategy, and cybersecurity strategy. Recognizing how these strategies connect is essential to understanding what drives the organization and how to align efforts effectively. Participants will learn the importance of ensuring cybersecurity is in sync with the broader organizational goals and how to make cybersecurity an enabler of digitalization and innovation efforts and create meaningful dialogues and collaborations across various business units. Based on the introduced frameworks, participants will later be presented with a key assignment in presenting a cybersecurity strategy that connects with their organization.

**Keywords:** Business Strategy, Cybersecurity Strategy, Digital Strategy, Innovation, Digitalization, Organizational Alignment, and Business Drivers.

**Outcome:** Participants will gain strategies to align cybersecurity with the digital agenda and broader organizational goals, positioning it as an enabler of business growth and innovation. They will learn to identify key initiatives that support these objectives while fostering collaboration across business units.

## Module 3: Enterprise Risk Management & Risk Quantification

This module provides participants with the knowledge to navigate the complex threat and risk landscape across the entire value chain. Emphasizing cyber risk within the broader enterprise risk management framework, the module focuses on clear and compelling communication to executives, aligning with business priorities and securing resources for mitigation. It also covers the development and frameworks to measure and report cybersecurity risks and progress in a way that resonates with executive stakeholders. Participants will explore methods for quantifying risks, assessing potential consequences, and leveraging e.g. Business Impact Analysis (BIA) as a key tool to prioritize and design effective risk mitigation strategies.

**Keywords:** Enterprise Risk Management, Cyber Risk, Risk Mitigation, Risk Reporting, Risk Quantification, and Business Impact Analysis (BIA).

**Outcome:** Participants will gain models to assess enterprise risks and think Business Impact Analysis into risk management practices. They will also learn how to map and prioritize cyber risk against enterprise risk in communication with senior executives.

# Modules & Learning Objectives

## Module 4: Business Resilience & Crisis Management

This module explores best practices in crisis management and business continuity, and how to ensure business resilience in crisis situations. It introduces models and plans for crisis response and disaster recovery, highlighting the importance of training, effective communication, clear ownership, defined escalation paths. The module provides inspiration on how continuous training can be done with simple practices and gamification to improve organizational resilience over time. Through a crisis simulation exercise, participants will test their ability to navigate a chain of events and maintain composure under pressure. They will receive feedback on their communication, collaboration, and leadership to increase self-awareness and improve techniques in leading through disruptions with minimal impact.

**Keywords:** Business Continuity, Crisis Management, Crisis Response, Disaster Recovery, Contingency Planning, Organizational Resilience, Crisis Communication, Continuous Training and Crisis Simulation.

**Outcome:** Participants will gain practical insights into crisis management and business continuity, learn how to foster a culture of continuous training to strengthen organizational resilience, and enhance their ability to lead through high-pressure situations with confidence.



## Get tools and strategies from insightful leaders inside and outside Cybersecurity

### Jens Rasmussen | Program Manager & Faculty Instructor

Jens is a senior executive advisor with over 25 years of experience across all areas of IT and digital transformation. As the former CIO of Chr. Hansen, and other leading firms, Jens has a proven track record in M&A and private equity, with extensive expertise in building and managing organizations and stakeholders.

With a background in Economics and Commercial Law from CBS, Jens brings a business-centric approach to the CISL program, focusing on balancing value creation with risk mitigation. As both an instructor and a program manager, Jens shares his deep knowledge of IT and digital strategy, management, and architecture, making significant contributions to topics such as stakeholder communication and enterprise risk management, ensuring high-quality delivery and coherence throughout the program.



## **Per Silberg | Program Manager & Faculty Instructor**

Per is a seasoned executive advisor and board professional with deep expertise in risk management, cybersecurity, and IT. With more than 25 years of experience and over 30 major crisis events behind him, Per has a strong track record of guiding boards, senior executives, and CISOs through complex challenges in organizations such as Sydbank, Ecco Sko, Bestseller, and Danfoss.

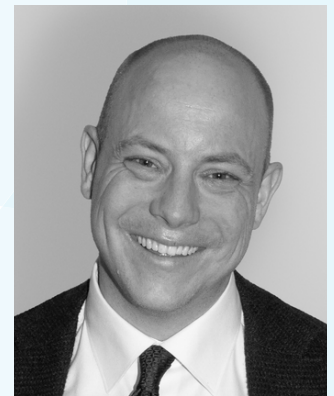
As Executive Advisory Partner at Monoceros, Per brings strategic security insight and hands-on crisis experience to the boardroom — translating complex cybersecurity challenges into business decisions that drive long-term value and resilience. As an instructor at Executive Cognito, he connects cybersecurity and risk management with board-level decision-making, equipping leaders with the perspectives needed to turn risk into opportunity.



## **Jakob Skytte | Faculty Instructor**

Jakob is a seasoned management consultant and executive advisor with expertise in organizational management—from strategy to execution—across cybersecurity, digital, and risk. As Founder and Partner of Copenhagen Consulting, Jakob has a strong track record of managing global and technical projects in critical industries, supporting senior executives through organizational transformation.

With a strong background in management consulting, Jakob excels at designing organizations for success and helping leaders navigate emerging risks and opportunities. As an instructor, Jakob plays a key role in connecting cybersecurity with organizational drivers, especially on Digitalization, sharing effective strategies and tools to sharpen conclusions and build alliances. Jakob has played an instrumental role in developing the CISL program and serves on the CISL exam board.



### **Camilla Treschow Schrøder | Faculty Instructor**

Camilla Treschow Schrøder is an experienced cybersecurity Headhunter and Founder of Treschow&Son, supporting clients in attracting, developing, and retaining top cyber talents from specialist to executive levels through recruitment and educational services. As a trusted advisor in cyber executive hiring, Camilla offers sharp insights into the evolving landscape of cyber leaders and the CISO role— illuminating key responsibilities, organizational structures, and personal characteristics that drive success.



With a strong track record in executive hiring and deep insights into the Enneagram, Camilla delivers practical strategies for identifying and developing leadership capabilities as an instructor and coach in the CISL Program. She is the Co-Founder of the CISL Program, and her company, Treschow & Son, is its exclusive provider.

### **Klaus Kongsted | Faculty Instructor**

Klaus Kongsted is a seasoned expert in Governance, Risk, and Compliance (GRC) bringing extensive experience in cybersecurity as both a consultant and business executive. As founder of Dubex, Klaus has honed his skills in cybersecurity and risk management, with in-depth knowledge of industry frameworks and standards. He is an active member of several councils, committees, and boards and has contributed to public recommendations on cybersecurity from the Board Association.



Active across governance, risk, and compliance, Klaus contributes to the CISL program on enterprise risk management, with a particular focus on risk quantification. As an instructor, Klaus presents a framework for risk quantification to strengthen communication on risk mitigation and management between cybersecurity and business executives. Klaus is the Co-Founder of the CISL Program and serves on the CISL exam board.

# Guest Speaker Portfolio



**Per Silberg Hansen**  
CEO, Monoceros Security



**Martin Kofoed Høding**  
CISO, SAS - Scandinavian Airlines



**Louise Hahn**  
CEO, Mind Energy



**Shehzad Ahmad**  
CISO, IF Insurance



**Thomas Mølgaard**  
Security Country Lead, Denmark  
DXC Technology



**Rasmus Rasmussen**  
VP Enterprise Platforms,  
Infrastructure & Security, Demant



**Martin Modvig Stausbøll**  
Partner, Kopenhagen Konsulting



**Anne Sofie Roed Rasmussen**  
CISO, Novonesis

”

The 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, CPH Airports A/S

”

If you want to learn what it is that drives your organization and improve your chances of overcoming challenges that extend outside of cybersecurity, the CISL program will offer you a safe playground to do so.

Søren Sloth, Senior Manager Infrastructure & Operations, Danish Crown



# 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 Spring 2027

**Module 1:** 3rd - 4th of February

**Module 2:** 24th - 25<sup>th</sup> of February

**Module 3:** 16th - 17th of March

**Training day:** 13th of April

**Module 4:** 4th - 5th of May

**Exam:** 1st of June

## Location

Single modules are held at Copenhagen Konsulting's headquarters in Nordhavn, Copenhagen. Residential modules are held at Holckenhavn Castle located in Nyborg

## Price & Registration

Price 68.000 DKK ex. VAT and covers:

- 9 full course days
- 3 leadership coaching sessions
- Accommodation & catering
- Materials

Price 88.000 DKK ex. VAT. including

- CISM exam training

To register for CISL click [here](#). Upon confirmation, the full price will be invoiced. For any inquiries regarding registration, please contact [cts@cisl.dk](mailto:cts@cisl.dk).

## 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. Requests will only be accepted in written form to [cts@cisl.dk](mailto:cts@cisl.dk).

Holckenhavn Slot,  
Holckenhavn 1, 5800 Nyborg

# 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**

3 yearly network events:

3 x 24-hour stayover meetings

Yearly membership fee: 16.000 DKK ex. VAT.

Includes accommodation and catering.

# Founders & Partners

## 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 Copenhagen Talent House 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.

## CISL Partners

CISL partners with experts in and outside the cybersecurity industry in creating a program that is practical, relevant and forward-thinking. Our partners support our mission to build resilient cyber leaders who can lead themselves, their teams and their organizations through the everchanging digital landscape.

## Kopenhagen Konsulting

We specialize in helping leaders navigate uncertain challenges and achieve strategic objectives through expertise in Cybersecurity, Digital and Risk. 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