

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

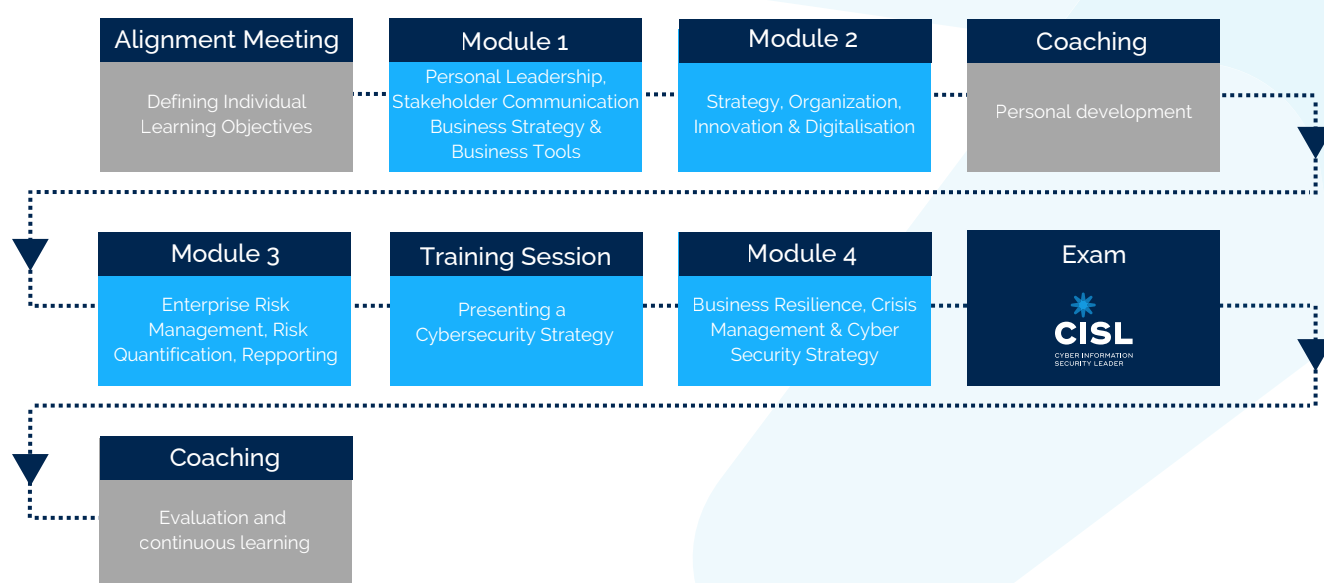
The program comprises of 9 full-course days. Course days are divided into 4 themed modules and a training session. Module 1 and 4 constitute residential courses to promote a strong network and to foster ongoing dialogue among participants.

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 3-day CISM exam training course preparing for a CISM certification through ISACA Denmark. For price information see: **Practical Information**.

Fig. CISL Program Overview



Modules

Module 1:

Day 1

Personal Leadership & Stakeholder Communication

This module introduces the foundations of personal leadership and effective stakeholder communication. Participants gain insight into how individual motivations and behavioural patterns influence collaboration, communication and conflict management. Using the Enneagram framework as a practical development tool, participants deepen their self-awareness and learn to identify different behavioural and communication styles among stakeholders. This enables them to adapt their communication, strengthen stakeholder relationships and increase their ability to engage, convince and influence others. The module serves as the foundation for participants' personal development journey throughout the programme. Based on the insights gained during the day, participants define individual development goals that will be further supported and refined through coaching sessions during the course.

Day 2

Strategy, Understanding the Organisation & Business Tools

This module introduces the fundamental principles of business strategy, key financial and business concepts, stakeholder management and enterprise architecture, providing participants with a broader understanding of how organizations are structured, governed and managed. Participants are introduced to basic financial concepts and learn how they influence business priorities, investment decisions and resource allocation. They are introduced to business case models and will through enterprise architecture principles gain an understanding of how business processes, technology and organizational structures work together to support business objectives. Through stakeholder management frameworks and exercises they learn how to navigate and influence stakeholder landscapes and communicate effectively across the business.

Module 2:

Day 1

Digital 2.0 and The role of AI

This module introduces participants to strategic thinking and the key elements of business strategy. Participants learn how to interpret strategic objectives, distinguish between growth and risk-related priorities. Participants learn how business strategy, digital strategy and cyber strategy align to support organizational objectives. The module examines how artificial intelligence is reshaping business models, decision-making and innovation, creating new opportunities as well as new risks. Participants gain an understanding of how security leaders can support digital ambitions and enable innovation while ensuring that security remains aligned with business priorities. The day also introduces practical approaches to prioritization, helping participants distinguish between urgent and important activities and focus efforts where they create the greatest organizational impact. In addition, participants learn how to structure and communicate strategic messages through effective PowerPoint presentations.

Day 2

Governance, Working with and reporting to the board & senior management.

This module introduces cybersecurity governance and the role of boards and senior management in overseeing cyber risk. Participants gain an understanding of executive priorities, decision-making processes and the governance structures that support effective risk management. Participants learn how to communicate cybersecurity topics to boards and senior management, including how to present risks, priorities and recommendations in a clear business context. The module also covers reporting principles and how to establish meaningful governance and oversight of cybersecurity activities. The day further explores how cybersecurity functions can be designed and organized to support business objectives. Participants gain insight into reporting lines, governance models, operating structures and resourcing approaches, and how these influence the effectiveness of the cybersecurity function as part of the broader organization.

Modules

Module 3:

Day 1

Risk Quantification and Transfer (Insurance)

Participants learn to identify what is truly critical to the business through Business Impact Analysis, mapping dependencies on processes, systems and suppliers. The day positions cyber risk within enterprise risk management and compliance requirements and shows how to turn business impact into clear priorities. Participants are introduced to best practices in third-party vendor management, including how to assess, monitor and manage risks related to suppliers and external service providers. This includes understanding supplier criticality, dependency mapping, risk ownership and the integration of third-party risk into the broader enterprise risk management framework. Finally, participants learn to structure risk reporting that resonates with top management and boards, enabling informed decision-making and effective governance.

Day 2

Enterprise Risk Management and Compliance

Participants learn how to assess and quantify cyber risk in business terms, enabling more informed decision-making and effective communication with executive leadership and boards. Using quantitative methods such as FAIR and annual loss expectancy, they develop realistic loss event scenarios and translate technical and operational risks into financial impact. The day explores how organizations define risk appetite and tolerance, evaluate risk treatment options and make risk-based investment decisions. Participants learn when to mitigate, accept, avoid or transfer risk, including the role of cyber insurance within a broader risk management strategy. In addition, participants gain an understanding of how risk quantification supports governance, compliance obligations and enterprise-wide decision-making, helping organizations align cyber risk with business priorities.

Module 4:

Day 1

Business Continuity Management, Crisis Management and Disaster Recovery

Participants learn how to prepare for, respond to and recover from disruptive events while maintaining critical business operations. The day explores the principles of business continuity, crisis management and organizational resilience, including crisis response structures, contingency planning, disaster recovery and effective governance during incidents. Participants gain an understanding of crisis communication, escalation paths, roles and responsibilities, and the concepts needed to communicate effectively with executive leadership during high-pressure situations. The day also covers how organizations develop, maintain and test contingency and crisis management plans, and how continuous training strengthens resilience over time. Through a crisis simulation exercise, participants apply these principles in practice, demonstrating business understanding, prioritization and decision-making in a rapidly evolving crisis situation.

Day 2

Building a Security Strategy.

This module brings together the key concepts, frameworks and tools from the programme. Participants apply their learning to develop a comprehensive cybersecurity strategy aligned with business objectives, digital ambitions and organizational priorities. Drawing on principles from governance, enterprise risk management, risk quantification, resilience, stakeholder management and business strategy, participants learn how to translate strategic objectives into a coherent cybersecurity roadmap. The module focuses on prioritization, investment decisions, operating models, governance structures and the practical initiatives required to support the organization's long-term objectives. Participants present and defend their strategy, demonstrating their ability to balance risk, resilience, innovation and business value while communicating recommendations clearly to senior stakeholders.

Faculty Instructors

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.



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.

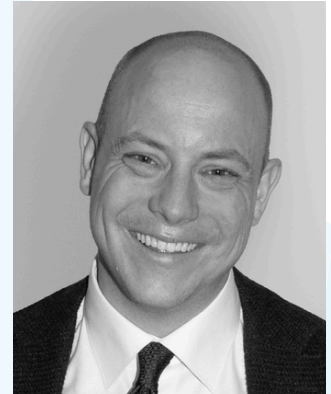
With a strong track record in executive hiring and deep insights into the Enneagram, Camilla delivers practical strategies for identifying and developing leadership capabilities as an instructor and coach in the CISL Program. She is the Co-Founder of the CISL Program, and her company, Copenhagen Talent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



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.



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 Erik Sørensen
Chairman



Per Silberg
Founder & CEO, Monoceros
Security



Louise Hahn
CEO, Mind Energy



Lars Falch
Partner, Kopenhagen Konsulting



Shehzad Ahmad
CISO, IF Insurance



Thomas Mølgaard
Security Country Lead, Denmark
DXC Technology



Rasmus Rasmussen
VP Enterprise Platforms,
Infrastructure & Security, Demant



Jonas Roos Christensen
Beredskabskoordinator, e - nettet



Martin Modvig Stausbøll
Partner, Kopenhagen Konsulting



Anne Sofie Roed Rasmussen
Deputy CISO, Novo Nordisk



Signe Behr - Rasmussen
Senior Advisor, Monoceros
Security



Christian Bränniche Lund
CISO, DSB

”

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 - 25th of February

Module 3: 16th - 17th of March

Training day: 13th of April

Module 4: 10th - 11th 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

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

Price 68.000 DKK ex. VAT

Including CISM exam training

Price 83.000 DKK ex. VAT.

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

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: 20.000 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

