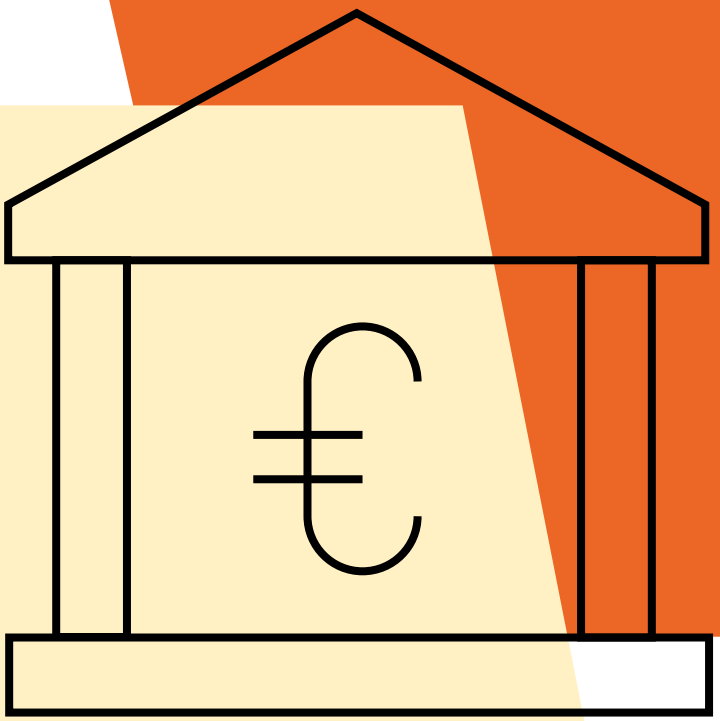
Certified
Path



Qualified Cybersecurity Professional in Finance

30.01.2025

Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT

febelfin academy

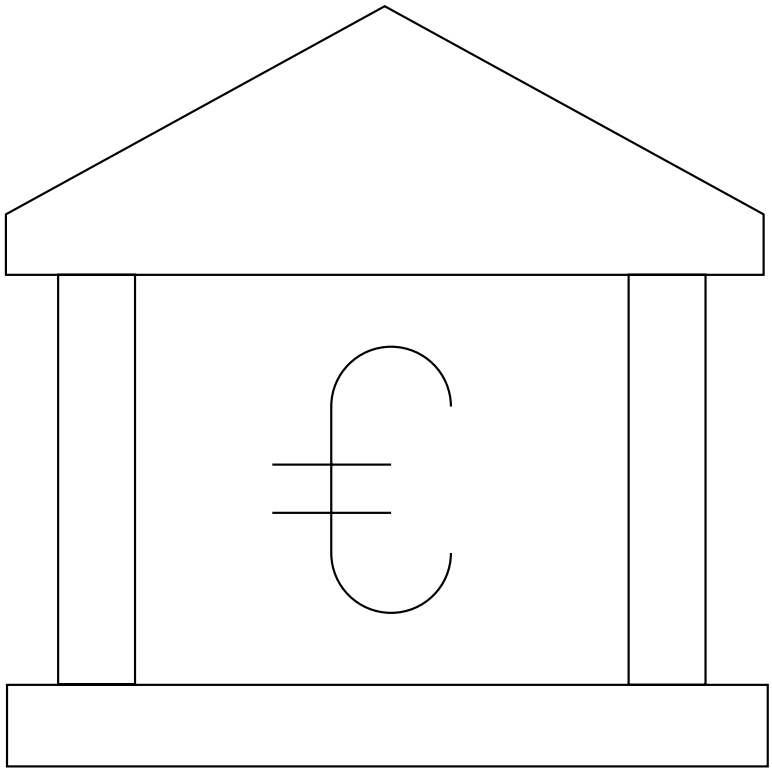
ABBL

HOUSE OF TRAINING

Cybersecurity Expertise for the Financial Sector

Our certified path "Qualified Cybersecurity Professional in Finance" is your gateway to mastering the intricate and critical domain where finance and technology intersect. In an era where financial institutions are prime targets for cyber threats, this specialised training is designed to empower professionals with the skills necessary to protect and secure the financial landscape.

In this unique collaboration, House of Training, ABBL, Febelfin Academy partners with Solvay Lifelong Learning, to deliver a programme tailored to the specific challenges and intricacies of cybersecurity in finance. The course brings together the regulatory insights and industry-specific expertise of ABBL/Febelfin Academy with Solvay's cutting-edge academic approach, ensuring participants gain a comprehensive understanding of cybersecurity in the financial domain.



HOUSE OF **TRAINING**

houseoftraining.lu

Audience and Objectives

Target Audience

The training course accommodates a diverse range of participants, catering to specific needs and roles within various industries. The course can be followed by various target groups:

- Finance professionals: already engaged in the finance sector, including financial analysts, managers, and executives, seeking to enhance their understanding of cybersecurity specific to financial environments
- Process & Business analysts
- Business managers in insurance companies or financial institutions
- Product managers
- Risk Managers
- Compliance Officers
- FinTech

Objectives

The objectives of the course are to:

- provide participants with the essential skills and knowledge required to navigate the complex landscape of cybersecurity within the financial sector
- tackle specific challenges faced by financial institutions, focusing on risk management, compliance strategies, and the protection of sensitive financial data
- foster an understanding of regulatory frameworks governing cybersecurity in finance, ensuring participants can align security measures with industry standards
- empower participants to analyse and respond to emerging cyber threats, incorporating threat intelligence into their cybersecurity strategies
- cultivate leaders in the field by fostering a strategic understanding of cybersecurity, enabling participants to proactively safeguard financial systems and contribute to the industry's resilience

Programme

The body of knowledge is aligned with the Executive Master in Cybersecurity management lectured at Solvay Lifelong Learning (solvay.edu/cybersecurity). It is based on material compiled by Professor Georges Ataya, as well as on general publications related to cybersecurity. The education is structured into four modules.

Lead speakers

Pr. Georges Ataya
Academic Director Digital Governance and Trust, Solvay Brussels School of Economics and Management

Pr. Georges Ataya has over 20 years of experience in education and training, particularly as the founder and Academic Director of the Digital Transformation, Governance and Trust program at Solvay Brussels School. He founded ICT Control in 1999 and has held various leadership roles in IT governance, cybersecurity, and data protection, including past International Vice President of ISACA.

Steve Purser
Independent Cybersecurity Consultant - CSPRO Services

Independent consultant with over 25 years' experience, specialising in strategic, regulatory, and technical aspects of cybersecurity. Former Head of Operations for the EU Cybersecurity Agency (ENISA) and CISO of several financial institutions. Member of several industry boards.

"I help organisations to adopt practical and cost-effective approaches to cybersecurity."

Module 1

Introduction to Cybersecurity Fundamentals

1 day - 6h classroom

30.01.2025

Guest speakers

Atefeh Maleki
Head of Information Security Department, Nomura Bank Luxembourg S.A.

Atefeh Maleki is currently leading the information security at Nomura Luxembourg. She has more than 10 years of experience in technology with a focus on cybersecurity and IT risk. Passionate about cybersecurity, she is a member of Women Cyber Force in Luxembourg.

Objective

This module aims to equip participants with a comprehensive understanding of cybersecurity principles, covering fundamentals, governance, risk, and compliance. It focuses on confidentiality, integrity, and authentication processes, emphasizing the protection of sensitive information and adherence to predefined policies. The curriculum includes in-depth risk management practices, guiding participants in identifying and mitigating cybersecurity risks effectively. Additionally, it addresses compliance and legislation, stressing the importance of adhering to industry standards. By the module's conclusion, participants will have a solid foundation to explore and specialize in cybersecurity confidently.

Module 2

Cybersecurity Battleground: Threats, Vulnerabilities and Technologies

1 day - 6h classroom

31.01.2025

Guest speakers

Antoine Meyers
CISO - BGL BNP Paribas

Objective

In this module we will comprehensively address cybersecurity management by integrating key capacities such as Identification, Protection, Detection, Response, and Recovery techniques. The curriculum presents current threats, vulnerabilities, security controls, and technologies, offering insights into the threat landscape.

It emphasizes the connection between cybersecurity and information security practices, aligning frameworks with business needs and risks. The course delves into existing frameworks, risk analysis, management buy-in, solution search, alignment with risk appetite, implementation, and follow-up.

Decision-making tools for adverse conditions and seemingly hostile environments are provided to participants. Additionally, a specific financial sector workshop is included, focusing on the identification of threats and vulnerabilities related to business functions, risk practices, and the determination of a robust mitigation model.

Module 3

Incident Response by security controls and operations

1 day - 6h classroom

27.02.2025

Guest speakers

Nicolas Bomont
IT Infrastructure Manager - Victor Buck Services, Luxembourg's leading business document management company. Since January 2021, member of Cybersecurity Advisory Network

"I put innovation and security to work for businesses and like transforming legal constraints into growth opportunities."

Objective

This module covers context analysis, scope definition, threat modelling, security controls, and solution space identification. Emphasizing a holistic approach, it explores trade-offs from technological, human, and procedural perspectives. The significance of kill-chain analysis in threat modelling is highlighted for focus, cohesion, and business case development. Operational planning tools and frameworks introduce defence theory, mental models for understanding adversaries, telemetry, attack detection, incident response, crisis communication, and continuous improvement assessment tools. In summary, the module provides a comprehensive guide to navigating security controls and incident response in operations.

Module 4

Cybersecurity -Governance Management - Leadership

1 day - 6h classroom

28.02.2025

Guest speakers

Lars Weber
Vice President & Head of Business Unit, Non-Financial Risk Management, Information Security Officer, BCEE

After his studies of “Computer Science” at the RWTH Aachen, Lars joined the IT security team of Spuerkeess in 2000. For several years, he was in charge of the « Operational IT Security » team. In 2019 he took over the role of “Information Security Officer” while joining the risk management department as “Deputy Head of Risk Management”.

Since 2023, He acts as “Vice President & Head of Non-Financial Risk Management” and “Information Security Officer” at Spuerkeess.

Objective

During this course, we will provide you with a thorough understanding of cybersecurity management, focusing on roles and responsibilities in crafting and executing a robust strategy. It emphasizes aligning strategic components with organizational goals and adapting to evolving threats, covering vital areas like supply chain considerations, the three lines of defence, and the seven components of maturity.

The module explores effective governance practices, including frameworks and policies, fostering a well-structured and accountable governance framework. Communication is highlighted as crucial for successful cybersecurity governance, empowering participants to convey policies, incidents, and strategies to diverse stakeholders, promoting cybersecurity awareness. Ultimately, participants gain the knowledge and skills needed to develop a comprehensive cybersecurity strategy, implement effective governance, and enhance communication within their organizations.

Exam

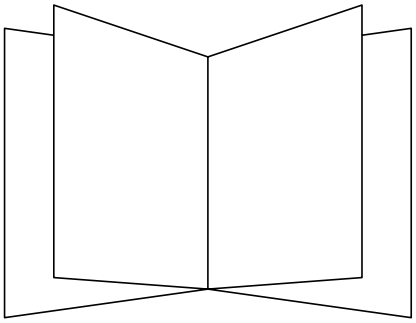
The knowledge acquired in the seminar will be validated through an examination. The examination is based on a MCQ questionnaire of around 30 questions. The required passing rate is 60%.

Certificate

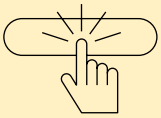
Candidates who successfully complete the examination will receive the following certificate of completion co-signed by the ABBL, Febelfin Academy, Solvay Lifelong Learning and House of Training: "Qualified Cybersecurity Professional in Finance".

Information & Registration

Information

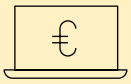


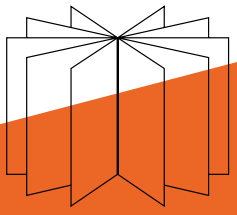
Registration & fees



Registration for the training modules and/or exams is to be made online via our website at least 5 days before the beginning of the training course/exam.

The fees indicated in this flyer represent the basic fees. They can vary, depending on several options chosen by the participant (training material, exam fees, etc.). All prices are indicated without VAT (3%)

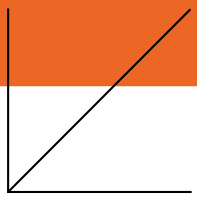




Training location

Unless otherwise indicated in the registration confirmation, all courses take place at the:

Training Centre in the Chamber of Commerce
7, rue Alcide de Gasperi
L-2981 Luxembourg



Contact

House of Training - Customer Service
customer@houseoftraining.lu
BP 490 L- 2014 Luxembourg
Tel.: +352 46 50 16 – 1

www.houseoftraining.lu

Terms and conditions as stated on our website www.houseoftraining.lu are applicable

Notes

Réorientation **OU** Perfectionnement

Tous vos choix mènent à la

HOUSE OF TRAINING

Des formations pour
une évolution professionnelle

houseoftraining.lu

HOUSE OF
TRAINING

houseoftraining.lu

customer@houseoftraining.lu