Qualified Cybersecurity Professional in Finance

GOALS

Welcome to the forefront of safeguarding the financial world in the digital age!

Our program "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 specialized training is designed to empower professionals with the skills necessary to protect and secure the financial landscape.

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

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.

This education program is directed by Professor Georges Ataya, Academic Director at Solvay Lifelong Learning. He is the co-founder and Vice-Chair of the Belgian Cybersecurity Coalition, past Vice President of the ISACA Research Foundation, and co-author of the Certificate in Cybersecurity Management.

SUMMARY

Category:

- Compliance & audit

Difficultylevel:

Advanced

Certification type:

In class training

Price:

The joint pricing guidelines are applied as part of a joint initiative.

CPD hours:

- Bank: **24h** general

- Insurances: **24h** general
- Consumer loans: **24h** general
- Mortgages: **24h** general

INTENDED 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
- …

FOREKNOWLEDGE

Advanced level training: this training requires a general basic knowledge of the subject.

Preparation:

We kindly ask you to study the pre-course material (available on your profile MYFA) before the start of the trajectory – some of them are a must read, others are optional to read. They have been carefully selected to introduce the class workshops and to support in-depth discussions with fellow participants.

- Module 1 : Cyber Security Incident Management Guide | Centre for Cyber security Belgium
- Module 2 : Good Practices for Supply Chain Cybersecurity — ENISA (europa.eu)

CONTENT

CONTENT

Curriculum: 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. This training is also recognised by The House of Training (Chamber of Commerce and the Luxembourg Bankers' Association (ABBL)). The education is structured into four modules.

Module 1 : Introduction to Cybersecurity Fundamentals ***(duration 1 day 6h classroom)***

Lecturers : Prof. Georges Ataya, Solvay Lifelong Learning
Guest speakers : Caroline Sellami, Financial Services and Markets Authority (FSMA), Management of public, institutional and strategic affairs and strategic projects.

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 (duration 1 day 6h classroom)

Lecturers : Taco Mulder, Solvay Lifelong Learning
Guest speakers : Xavier Neerdaels, Chief Information Security Officer BNP Paribas Fortis

***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, Security Controls and Security Operations (duration 1 day 6h classroom)

Lecturers : Taco Mulder, Solvay Lifelong Learning
Guest speakers : Johan Klykens, Director - Centre for Cybersecurity Belgium - Certification

***Objective**:* This module covers context analysis, scope definition, threat modeling, 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 modeling is highlighted for focus, cohesion, and business case development. Operational planning tools and frameworks introduce defense 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 (duration 1 day 6h classroom)

Lecturers : Prof. Georges Ataya, Solvay Lifelong Learning
Guest speakers : Alexandre Pluvinage, Head of Fraud and Online Security Awareness ING

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 defense, 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.

PRACTICAL INFORMATION

- **Duration:** 4 days of training (6 class hours per day)
- **Hours:** 09:00 to 17:00
- **Location:** Febelfin Academy: Phoenix building, Koning Albert II-laan/Boulevard du Roi Albert II 19, 1210 Brussels
- **Language:** This training will be given in English.
- **Preparation:** We kindly ask you to study the pre-course material (available on your profile MYFA) before the start of the trajectory – some of them are a must read, others are optional to read. They have been carefully selected to introduce the class workshops and to support in-depth discussions with fellow participants.
- **Qualification and examination information:** The program leads to the certification "Qualified Cybersecurity Professional in Finance" at the conclusion of the full program and after succesfully completing the corresponding tests.
    - The tests for module 1 & 3 at the end of the course consist of multiple-choice questions (no disc correction). These tests are made remotely at your (work)place. One must complete the online-tests within a month of taking the training. You have 2 attempts to pass these tests.
    - The tests for modules 2 & 4 consist of group assignments and are administered in class during the scheduled sessions. These cannot be retaken.
    - For a satisfactory result, you must obtain at least 60% for each module. If you pass, you will receive the certificate proving that you have passed the tests and that you have the required technical knowledge.

METHODOLOGY

You follow a **'Classroom training'** in a group. You, the other participants and the teacher are all present in the same classroom at an agreed time. There is an opportunity for interaction and feedback, both from the participants to the teacher and vice versa. The teaching material consists as a basis of a presentation via the MyFA learning platform, supplemented with various other items (such as digital syllabus, presentation, audiovisual fragments, etc.).

Training material:

- PowerPoint slides
- Various pre-course materials