ULB Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT

DIGITAL GOVERNANCE AND TRUST | **DURATION** 12 MONTHS | **LANGUAGE** EN | **LOCATION** BRUSSELS

EXECUTIVE MASTER IN

CYBERSECURITY MANAGEMENT

Information Security, Cybersecurity and Digital leaders have been counting on Solvay Lifelong Learning in getting the necessary knowledge and skills for boosting their careers.

The second edition of Executive Master in Cybersecurity Management starts in January 2024 with an innovative and effective hybrid learning model. Accessible to qualified participants from all over Europe, the program offers a flexible curriculum and hybrid study model making it possible for participants to combine classes with a full-time professional activity.

This Executive Master, delivered by a leading European Business School, holds various international and Belgian accreditations. The program is structured around six modules with a rich curriculum and innovative learning model, as follows:

- Guided self-study supported by recommended reading materials, and online coaching sessions
- Advanced lectures from leading experts during 2 in-person days on campus per each module
- Group case study activity with peers from various European countries
- Case study report delivery following your intense group effort

Modules are directed by senior practitioners and classes are lectured by leading cybersecurity experts. The education is mapped against major frameworks and bodies of knowledge including ENISA Cybersecurity Skills. Information Security and Cybersecurity leaders have relied on Solvay Lifelong Learning since 2003. Join hundreds of our successful alumni who boosted their careers after following our courses!

Georges Ataya
Academic Director

THE PROGRAMME AT A GLANCE

This programme is designed for professionals requiring managerial and practical knowledge of the six domains representing the pillars of cybersecurity activities and management practices.

IN BRIEF

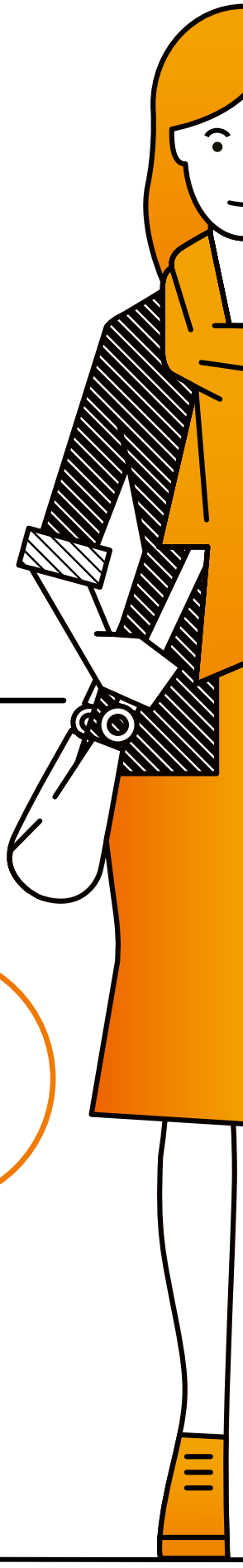
INSTITUTIONAL PARTNERS

ISACA Belgium Chapter · CISO · WOMEN 4CYBER · BOSA Federal Public Service Policy & Support · DPO CIRCLE · economie · ECS · CYBER SECURITY COALITION · .AGORIA

SPONSORING PARTNERS

DXC TECHNOLOGY · proximus ada · Orange Cyberdefense · Skillsbeam · sopra steria · LEONARDO · its me · HTP · Microsoft · AP · WAVESTONE · NTT DATA

YOUR BENEFITS



Boost your Cybersecurity management career and focus on essential domains of knowledge and practice.

CAREER BOOSTER

YOU.

EXTENDED KNOWLEDGE

The program is mapped against major bodies of knowledge, including the ENISA Cybersecurity Skills framework.

Accessible across Europe with a hybrid educational model, designed for cybersecurity professionals. Combine this engaging study experience with your current professional activity.

HYBRID, ACCESSIBLE EDUCATION

COMBINATION OF
6 BODIES OF KNOWLEDGE

The Executive Master in Cybersecurity Management addresses the following six domains of knowledge that are essential for Cybersecurity and Information Security Leaders.

1

January to February 2024

INFORMATION SECURITY LEADERSHIP

The CISO Fundamentals

Topic leader : Marc Vael

The core management activities of a modern information security leader include security governance, risk management, program management and incident management processes. This module illustrates job description of a typical CISO today and the role of a CISO at an organisation, explaining reporting lines and responsibilities, skills, and expertise. In this module we will talk about typical challenges that CISOs face in their role. This module also addresses design and implementation of an Information Security Strategy taking into account an assessment and relevant information security risks. Proper attention will be given to application of the information security management system (ISMS), proactive and reactive security incident management as well as tracking security leadership KPIs. Finally, this module will focus on self-evaluation of a CISO. Pre-readings for this module include ISACA CISM body of knowledge, ISO 27xxx security standards, NIST Cybersecurity Framework, ISACA Digital Trust approach, Hofstede cultural dimensions theory. At the end of the module participants will be working in groups on development of a new security strategy and improving current security of an organisation as a part of their business case.

2

March to April 2024

SECURITY CONTROLS

Governance, Risk, Compliance and Certification

Topic leader : Wim Bartsoen

This module will take participants through the process of analyzing context, defining scope, modeling threats, outlining security controls and requirements, finding the solution space for controls (incl. technologies and operating models), evaluating risk (Inherent vs. Residual) and anchoring it in policy, providing assurance that controls operate as intended for the purpose of internal and external assurance obligations or certifications. This part builds on concepts introduced in module 1 (Information Security Leadership). Participants will gain a good understanding of security controls and their respective trade-offs from the angles of technology, people, and process. They will understand how kill-chain analysis in threat modeling helps bring focus and cohesion, and how it also helps in building a business case. They will gain an understanding on how a layered approach of assurance and reporting supports effective management of security controls. Pre-readings for this module introduce participants to various control frameworks such as COBIT, ISO 27002, NIST cybersecurity controls, CIS20 and OWASP models. During the group case work participants will focus on practical application of threat modeling techniques, control specifications, governance definition and operations in an enterprise focusing on crown jewels.

3

May to June 2024

SECURITY ARCHITECTURE

Securing the Landscape

Topic Leader: Eric van Zuuren

Often people talk about “security-by-design” or “privacy-by-design”. Indeed security cannot be “bolted on” effectively at a later stage. The better security is embedded “by design” in all layers of your organization’s solution architecture, design and delivery, run and operations, the better you will be able to understand your security posture, as well as outstanding gaps and risks. To understand all the benefits this module will demystify security architecture and explain how it can and should be used not only by IT professionals but also, how it can help support governance, risk and compliance processes. Participants will learn about various models of security architecture, how they can be effectively used to identify attacks vectors, threats and how these can be used to determine mitigating controls. Initial pre-readings include the TOGAF, SABSA, and OSA frameworks, followed by lectures with experienced speakers, and studying on concrete and practical cases.

4

September to October 2024

SECURITY OPERATIONS

Continuity and Crisis Management

Topic Leader: Remy Knecht

This module will build upon concepts of the previous modules where Information Security Governance, implementation of Security Controls and Secure Architecture are key building blocks to set up a good Security Operations team. Information technology has become critical for most modern businesses, as a result a cyber risk has become a business risk. Security Operations teams are facing today more pressure than ever to help manage the risks by identifying and responding to threats across a diverse set of technical assets, business processes, and users in a pro-active and reactive way. This module will teach how to design defences around unique organizational requirements and potential risk profiles. We will give you the necessary tools to build an intelligence-driven defence, measure progress towards your goals, develop more advanced processes like threat hunting, active defence, and continuous Security Operations assessment. Participants will gain a good understanding of the core and auxiliary functions of a Security Operations team and possible implementation models depending on an organization`s size and characteristics. The module will provide tools and frameworks for operational planning that will focus on key aspects like defence theory and mental models to understand and map potential adversaries, telemetry and analysis, attack detection and investigative process, incident response and crisis communication up to assessment tools and frameworks to strive for continuous improvement.

5

September to October 2024

CYBERSECURITY BATTLEGOURND

Threats, Vulnerabilities and Technologies

Topic Leader: Taco Mulder

Cybersecurity management practices require the knowledge of your own business, its functional and technical vulnerabilities and the threat landscape that needs to be addressed. The capabilities that require building cybersecurity capacity include Identification, Protection, Detection, Response and Recovery techniques and processes. This module will address day-to-day implementation of cybersecurity and information security, linking theories and practices, and explaining how to link frameworks with business needs and risks in a day-to-day environment. This covers knowledge of existing frameworks and risk analysis, as well as getting management buy-in, searching for adequate solutions that are aligned with a risk appetite, implementing and following-up. Participants will be given tools that will help them make decisions in adverse conditions and seemingly hostile environments. The case study involves implementation of cybersecurity in a business environment where stakes are high and where board and company security knowledge is limited.

6

Spread over the year

CYBERSECURITY GENERAL MANAGEMENT

Digital and Cybersecurity Leadership

Topic Leader: Daniel Lebeau

This module will take participants through the basics of General Management dedicated to Cybersecurity and Digital professionals. There will be four parts: Finance, Strategy, Leadership and Human Capital. In the first part participants will better understand the art and the language of finance. Topics that should be reviewed are the challenges of the income statement, balance sheet, cash, financial ratios, return on investment and working capital. In the second part fundamentals of business strategy will be introduced: SWOT analysis, types of strategy, strategic moves, seeking alignment to strategy in the implementation. The third part will be dedicated to how to build a team's self-confidence, encourage smart risk-taking, manage others with tough empathy, and give credit to others for their success. The last part is devoted to the growth of the human capital through smart recruitment, skills assessment, on-going training and performance evaluation.

ADJUSTED TO YOUR OWN NEEDS AND CAREER TARGETS

- A career development tool is available to participants in order to identify strong and weak skills based on their own self-assessment and the role that they select.
- Based on the survey results, participants adjust their efforts to focus on those domains that they require the most for the target role.
- As a result, both phases 1 (Acquire) and 4 (Case study) are required to address those focus areas.
- An acceptance interview is conducted with each candidate to assess your “fit” with the program, define your goals and motivations to join the program, and outline a study plan.
- Another interview is conducted before graduation to evaluate improvement on those skills that were identified as weak by participants.

Georges Ataya
Academic Director

The programme ensures that we not only understand our body of knowledge, but also practice it."

My expectations were high. I knew already that it would be something advanced but it took me by surprise how great it is to be among these top level cyber managers and experts. You get to meet a lot of people who work in the field that otherwise you wouldn't. I get to spend time with the best of the best in the cyber world and learn a lot. Definitely worth applying for the programme. I manage to do it from Montenegro so everything is possible!

Denisa Kurtagic
Threat Analyst
Ministry of Defense of Montenegro

I was blown away by the quality presentations and experience of exceptional peers who shared their insights. The experience left me feeling inspired and empowered, and I'm grateful for the opportunity to learn from such a talented and accomplished group of professionals. If you're interested in cybersecurity management, I highly recommend considering the Executive Master in Cybersecurity Management programme. The caliber of speakers and the depth of knowledge offered are truly unparalleled.

S.C.
CISO and DPO
Davinsi Labs

HYBRID EDUCATION METHOD

Each module is delivered in two months through self-paced studying and in-person classes (2 full days on campus every 2 months). Blended Learning method is applied for each module as follows:

1

ACQUIRE

part entails 3 offline weeks of pre-reading guided by a coach and 4-8 hours of self-learning per week. Participants have access to recommended pre-reading materials, ISO standards, PERLEGO, ISACA membership with several hundred books, articles and bodies of knowledge to complete the "Acquire" part.

2

EVALUATE

part consists of a short questionnaire to check the progress of preparations for 2 full days classes on-site.

3

BUILD

part entails attending classes and workshops during 2 full days on campus, led by an experienced coach and guest speakers who are leading cybersecurity experts.

TEACHING FACULTY

Academic team:

Georges ATAYA
Academic Director
Professor at Solvay Brussels School
Vice-President of the Cybersecurity Coalition

Frédéric ROOS
Deputy Academic Director

Topics Leaders:

Wim BARTSOEN
Chief Digital Security Officer at Securitas Group

Remy KNECHT
CSO at ITSME

Daniel LEBEAU
Former Group CIO
Senior Vice-President
Business Services at GSK

Taco MULDER
Chief Information Security Officer at FOD BOSA

Marc VAEL
Chief Information Security Officer at Esko, X-Rite and Pantone

Erik VAN ZUUREN
Founder of TrustCore.EU

4

PRACTICE

part entails working together on a group case study with group peers (small groups of 3-5 people). Thanks to the knowledge acquired during each module and phase, participants create/develop their own management reports to resolve the case study challenges.

5

DELIVER

during this phase participants present their module case study with group peers. At the end of each module participants take a multiple-choice questionnaire for evaluation of acquired knowledge during the module.

PRACTICAL INFO

DURATION
From January to December 2024

SCHEDULE
Hybrid Education:
- Combination of self-paced studying and in-person classes (2 full days on campus every 2 months).

LANGUAGE
English

LOCATION
Online & classes on campus
Solvay Brussels School (ULB, campus Solbosch)
Avenue F.D. Roosevelt 42
1050 Brussels

PRICE
12.950€
+350€ for acceptance & registration fees

DIPLOMA
The Executive Master in CyberSecurity Management holds accreditations from EQUIS, Qfor, and KMO Portefeuille. Upon completion of the programme, graduates will receive a University Certificate awarded by ULB, recognising their achievement.

ADMISSIONS CRITERIA:
- At least 5 years as a digital or cybersecurity manager.
- Actively involved in digital or cybersecurity activities and decision-making.

CONTACT US

ALINA KOBAL
Programme Manager
+32 (0)2 894 13 31
alina.kobal@solvay.edu

HOW TO REGISTER?
Surf to www.solvay.edu/cybersecurity

A PORTFOLIO OF PROGRAMMES TAILORED TO YOUR TRAINING NEEDS

COMPANY SPECIFIC PROGRAMMES

We can tailor the content of each programme and offer it as specific training organised within your company. We adapt it to the demands of your teams and your specific sector of activity.

More info?
csp@solvay.edu

Solvay Lifelong learning offers a full range of programmes to meet your needs throughout your professional career: general management, strategy, finance, taxation, marketing, innovation, entrepreneurship... Discover our complete range below.

EXECUTIVE EDUCATION

Short, medium and long courses in various fields, in English and French. For professionals seeking to upgrade their skills, advance their career and successfully manage businesses of all sizes.

General Management

- Executive Programme in Enterprise Risk Management
- Executive Master in Management
- Accelerated Management Programme
- Executive Programme en Management et Philosophies
- Sustainability Fundamentals
- Executive Master in Sustainability Transformation
- Executive Programme en Gestion de la Réputation

Digital Transformation

- Executive Programme in Business Analytics
- Executive Master in Cybersecurity Management
- Digital Impact for Finance Professionals

Marketing

- Executive Master in Digital Marketing and Communication

Leadership

- Leading Authentically in Digital Times
- Leading through Empowerment
- Programme in People Leadership
- Leading with Impact and Purpose

Finance & Tax Management

- Finance pour Non-Financiers
- Finance for Non-Financial
- Executive Master en Gestion Fiscale
- Modular Education in Finance

Solvay Entrepreneurs

- Boost & Get Ready
- Start & Suceed
- Lead & Grow

Specific Industries

- Executive Master in Future-Proof Real Estate
- Executive Master in International Association Management
- Executive Master en Management des Institutions de Santé et de Soins

ADVANCED MASTERS

Designed as full-time programmes for one academic year for Master students with no or limited professional experience (max 3 years). With the right mix of theory and practice, they prepare you for the job market.

- Advanced Master in Financial Markets
- Advanced Master in Innovation & Strategic Management
- Advanced Master in Biotech & MedTech Ventures

EXECUTIVE MBA

18 months programme for experienced professionals looking for a career change or a career boost. EMBA offers you the tools and insights you need to lead your transformation.

EXECUTIVE MASTER IN
CYBERSECURITY MANAGEMENT

www.solvay.edu/cybersecurity

Université libre de Bruxelles
Avenue F.D Roosevelt 42 - CP114/01
1050 Brussels, Belgium
Tel. +32 (0)2 894 13 31
alina.kobal@solvay.edu

DREAM. LEARN. LEAD.

Established in 1903, Solvay Brussels School of Economics & Management is a faculty of the Université libre de Bruxelles. It currently holds a leading position in Europe for research and education in the fields of Economics and Management. The school's core mission is to train business leaders and entrepreneurs with the ability to adapt to the ever-changing nature of Society and to shape tomorrow's world.

Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT

ULB