IT Security & Risk Management Programme

Gaining Competitive Advantage with an Optimal Risk Management in Cybersecurity

Programme designed in collaboration with Securitymadein.lu (SMILE) and placed in the framework of the Cybersecurity Week Luxembourg

Organisation sheet

Context And Objectives	Banks and other financial institutions face major cyber threats. Whatever their size, they are extremely attractive targets. They must invest in technical and organisational means to protect their business and clients. Banks need also to develop broader strategies to engage with governments, other banks, their clients and the public. This will be even truer as fintech develops and more complicated digital systems increase inter-connectivity, and therefore vulnerabilities. The only efficient way to address this issue is to adopt proper Security Risk Management practices to ensure the right investments are made. A major objective of this session is to make the link between Cyber and Risk Management to guide banks to face Cyber Threats. By the end of this week you will be able to: 1. Identify how Cybersecurity fits in the governance of your institution; 2. Make the right decisions on how to address the cybersecurity risks; 3. Know where to focus investment into security (have the information needed to decide where to invest resources and where to get started); 4. Know how to get started with risk management 5. Know how to set up security and defense controls 6. Know how to respond to security incidents 7. Know how to react under attack and 8. Be prepared for the worst. During this week, you will also be challenged to try to answer to the following questions: • What is the purpose of CyberSecurity? • Why is it important? • How to manage security?
Methodology-format	This seminar is placed on the context of the CYBERSECURITY week Luxembourg. It will apply a learning by doing approach that will help you to make the right decisions when you back in your own daily business. Interactive programme combining lectures, peer to peer workshops (creativity, defence controls scenario), case studies, serious games (Cyber attack simulation, Risk Management tool) and visits.
Target group	Executive levels, directors and managers of IT and information security, risk and compliance directors, managers of audit functions of financial institutions, central banks or supervisory bodies a partner country.
Language	A sound level knowledge of English is required as the programme will be delivered in English, without translation.
Experts	Practitioners of cybersecurity from the Luxembourg banking sector, experienced experts from SMILE (Security MadeinLux).
Location and Dates	Luxembourg during the Cyber security week. 5-day seminar - From 14 to 18 October 2019

IT Security & Risk Management Programme
Gaining Competitive Advantage with an Optimal Risk Management in Cybersecurity

CONTENT

Day 1 – 14/10/2019 - IT Security & Refresh

- Welcome
- Setting the scene & introduction
- Practical examples
- Basics 1-0-1
- Overview of the cybersecurity ecosystem in Luxembourg
- Governance, regulation, legal aspects
- IT–security vs. risk management

DAY 2 - 15/10/2019 - Cyber defence strategy based on a risk management approach, in line with the risk appetite of the Board - learning by doing

- Cybersecurity challenge
- What are the asset to be protected
- Information Security Governance
- Information Security Risk Management
- Workshop on specific risk scenario
- Optimised Risk Analysis Method & Platform
    - Introduction to the MONARC Tool – method for the optimization of risk analysis CASES (Cyberworld Awareness and Security Enhancement Services) https://securitymadein.lu/tools/monarc/

DAY 3 – 16/10/ 2019 - Cyber-attack simulation exercise including discussion with members of CIRL

- Cyber-attack simulation game - ROOM 42 (SMILE) & Discussion with members of CIRL - Computer Incident Response Center https://www.c-3.lu/room42/ & https://www.circl.lu/
- Visit to the Luxembourg House of FinTech (LHOFT) - https://www.lhoft.com/

DAY 4 – 17/10/2019 - State of the art and best practice workshops

- IT audit and Governance, Alain Blondlet
- AI Risk/Control, Emilia Tantar
- Cloud for banks? What to do and how? By the CSSF (Commission de Surveillance du Secteur Financier) - Supervisory Authority of the Luxembourg Financial Sector, David Hagen
- Initiating the journey into the Cloud - Cloud case study by a major insurance company, Michaël Frippiat

- Social Event « Cyber Challenges 2020 » organised by a Luxemburgish IT services company in the framework of the Cyberweek.

DAY 5 – 18/10/2019 – Application of the knowledge acquired

- Workshop in the framework of Cybersecurity4success, by the ABBL – The Luxembourg Bankers' Association
- Closing

Remark: By delivery date, any training documentation shall be subject to regular reviews and updates amending the table of content as described herein.

One of the core values of the House of Training is pragmatism, the training it provides is therefore: practical, current, modular and targeted.
Bank and finance professionals from all disciplines are facing one international challenge in particular, which is to work together to improve the quality of services while reducing costs, within a framework that is increasingly subject to strict regulations and the use of technology.

In order to face the challenge of delivering fully-adapted training programmes, the House of Training uses a quality management method that it calls "Quality Circles", that bring together professionals and practitioners from the financial sector with shared goals, philosophy and passion for learning. Our quality circles have an intimate knowledge of the real needs in the industry and collaborate actively with the House of Training to integrate this understanding into our programmes.