HOUSE OF TRAINING

ATTF LUXEMBOURG

Cyber and Information Security Management

Online Training

Organisation Sheet

Objective	At the end of this course, the participants will have an overall view of Cybersecurity and the problems related to this subject, which will allow them to guide their choices and their mission taking into account the risks associated with cyber security.
	
	To this end, by the end of the course they will have
	• covered the various areas of Cyber Security
	• obtained notions of user safety - individual behavior (passwords, email, mobility, social networks) and basic notions of Cyber-Security
	• obtained answers to the following questions:
	  • What is the purpose of CyberSecurity?
	  • How to manage security?
	  • What are the security and defense controls?
	  • What are the means to respond to security incidents?
	• understood how an attack is performed
	• Reviewed the context of regional security and regulation and the specificities of the financial field (PCI DSS, mBanking, eBanking)
	• reviewed ethics and standards related to Cyber Security

Methodology	Interactive Online Sessions of 3 hours with Q&A, exercices and debates ...
Audience	**Bankers located in North Macedonia** **Training** (8 sessions of 3 hours) - Directors and managers of banks, financial institutions, central banks or supervisory bodies in the areas of banking, such as IT, security, risk and compliance.
Language	English
Participants	15 participants (maximum)
Expert	Jean-Hubert Antoine, certified CISSP, CISM, C|CISO, CEH, ISO27005 Risk Manager, ISO27001 Lead Implementer, ITIL V3; Trainer CISSP, PECB (ISO27XXX) and Security Awareness 27 years of experience in IT, specialist in Cyber-Security, 12 years of experience in teaching

Organized with the support of

THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG

HOUSE OF TRAINING

ATTF LUXEMBOURG

Dates	8 sessions of 3 hours in 2 weeks (4 sessions per week). Total of 24 hours February 15, 16, 17, 18, 22, 23, 25 and 26, 2021 from 09.00 to 12.00

HOUSE OF TRAINING

ATF LUXEMBOURG

Cyber and Information Security Management
Online Training
Content

1. **Treats and Attacks**
   - What are the threats?
   - Understand how an attack occurs
   - Attacker profiles
2. **Information Security Basics**
   - What is the purpose of Cybersecurity?
   - Basics: Basic Triad, Notions of Risk, Threat, Vulnerability, Impact
   - The return on investment of security
   - Security Lines of Defense
3. **Information Security Management and Governance**
   - How to manage security?
   - Roles and Responsibilities
   - Security Controls
   - Security Policies
4. **Audits and Tests**
   - Security Audits
   - Security Testing
   - Pen Tests
5. **Security Incident Management**
   - How to manage Security Incidents
   - Security Operation Center (SOC) -Computer Security Incident Response Team (CSIRT)
   - Crisis Management
6. **Software Security**
   - Software development and application security
   - Software Security Testings, xAST
   - DevOpsSec
7. **Cloud and Mobile Security**
   - Cloud Security Controls – CASB
   - Mobile Device Security
8. **Security Awareness**
   - User security concepts -individual behavior
   - Methods