HOUSE OF TRAINING

THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG

ATF LUXEMBOURG

Seminar for Bankers in Macedonia, Skopje, February 5 - 7, 2018

Cyber and Information Security Management

Organization 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 seminar, group work, debates ...
Audience	Executives or 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, CDPO, CEH, ISO27005 Risk Manager, ISO27001 Lead Implementer, ITIL V3; Trainer CISSP, PECB (ISO27XXX) and Security Awareness 24 years of experience in IT, specialist in Cyber-Security, 11 years of experience in teaching
Dates	February 5-7, 2018 for 3 days

Seminar for Bankers in Macedonia, Skopje, February 5 - 7, 2018

Cyber and Information Security Management

Content

DAY 1
AM:
• What are the threats?
• Understand how an attack occurs
• Attacker profiles
PM:
• What is the purpose of Cybersecurity?
• Cybersecurity Basics: Basic Triad, Notions of Risk, Threat, Vulnerability, Impact
• The return on investment of security

DAY 2
AM:
• How to manage security?
• Security policies
• Ethics and Standards
PM:
• Security Incident Management
• Security Operation Center (SOC) -Computer Security Incident Response Team (CSIRT)
• The specificities of the financial sector (electronic banking, mBanking, banking, interconnection ...)

DAY 3
AM:
• Infrastructure and communication security
• Software security and Attacks
PM:
• User security concepts -individual behavior
(password, email, mobility, social networks)
• Conclusions