Cyber security for Risk Managers

GOALS

The goal of this course is to:

- review the key threats for the financial sector regarding cyber security;
- give an overview of the counter measures that are recommended in case of a cyber attack;
- introduce the different external compliancy requirements for the financial sector;
- explain how to use the ISO27005 framework for risk assesment;
- integrate information security into operational risk management.

SUMMARY

Category:

- Risk, finance & treasury
- Compliance & audit

Difficultylevel:

Expert

Certification type:

In class training

Price:

- Member: € 570.00
- Non member: € 685.00
- Partner BZB: € 570.00
- Incompany: custom tailored, prices on demand

INTENDED AUDIENCE

The training course can be followed by junior risk managers, internal and external auditors, treasurers and corporate financial professionals.

FOREKNOWLEDGE

Expert level training: this training requires thorough prior knowledge of the subject.

CONTENT

CONTENT

- Introduction
  - Review of key threats for the financial sector, based on industry reports and incidents made public.
- Cyber war game
  - We will apply the concepts explained previously to a specific scenario, which participants will need to solve in a crisis

management game. The scenario features a realistic attack. Round after round, participants (which each have to take on a defined management role) act as the executive committee of the company and must process the information received and make the decisions, hoping that these will help control the attack and minimize business impact. At the end of the game, an explanation of the attack and the related mechanisms is given, and a brief summary of the counter measures that are recommended is provided – so that participants gain a concrete set of examples of how security controls can juggle an attack.

- Information Security Compliance landscape for the Financial Sector
  - Introduction to the different external compliancy requirements for the Financial sector as well as tips & tricks on how to ensure (internal) compliance. We will also touch upon the impact of the EBA guidelines, the GDPR and the NIS on Cyber Security.
- Risk Assessment for Cyber Security
  - Starting from the ISO27005 framework, we will introduce a typical methodology for information security risk assessments, as well as briefly touch upon other known methodologies.
  - We will complement this theoretical introduction with two examples of risk assessment methodologies, one for a web application, and another for a third party supplier. There, we will introduce key security frameworks available to the risk manager to design an approach that addresses state of the art security controls exhaustively (e.g. ISO27002, CSA questionnaire, …) or select key controls to address most prominent risk areas (e.g. 20 critical security controls).
- Integrate Information Security into Operational Risk Management
  - This session will focus on how to integrate Information Security in the overall Operational Risk Management process, from a methodology and governance point of view.

PRACTICAL INFORMATION

- **Duration:** 1 day of training (6 class hours)
- **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

METHODOLOGY

You follow a **'Classroom training'** face-to-face 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 presentation