Cyber security for Risk Managers

GOALS

The goal of this course 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:

Blended learning

Price:

The joint pricing guidelines are applied as part of a joint initiative.

INTENDED AUDIENCE

This course brings value to junior risk managers, internal and external auditors, treasurers and corporate financial professionals.

FOREKNOWLEDGE

Expert level: This training will provide advanced characteristics on a specific topic. In order to grasp the concepts of this training, thorough knowledge is required (enhancement).

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 training

Hours: 9h - 17h (6 lessons per day)

Location: This training will be given online.

Additional information:

How do you start the webinar? You will receive a login and password by email to access our platform. In the platform you will find a link. By clicking on the scheduled date the webinar will start via Webex.
In order to receive training points, it is important to enter your own name and surname in Webex, follow the entire training day and answer the questions suggested by the trainer. Do not follow the training with several people on the same PC.

METHODOLOGY

Type of training:
During Live Webinars you see the presentation and the trainer live via your screen. You can communicate with the trainer and ask questions.

Training material

- PowerPoint presentation (slides);
- Live Video.