Module II.3519

Risk management and Audit

Person in charge: Matthieu MANCENY
Prerequisite: II.2317 / II.2417 Cybersecurity
Organization: Lectures and case studies
Evaluation: Exams, presentations
ECTS: 5 credits

Context

This module is a follow-up to the II.2317 / II.2417 Cybersecurity module, which allows students to gain a global understanding of the systems to be secured, whether at network level, information system or application development. This involves studying how to anticipate the risks involved in the system and how to react in the event of attack.

The management of a cyber crisis encompasses many points: definition of the actions to be taken to resolve the crisis, coordination of actions, communication with the concerned persons and organizations. Risk management aims to anticipate these crises by identifying the vulnerabilities of a company, assessing the risks involved, and raising staff awareness of safety issues. An audit can be carried out by experts (regarding rules of installation, deployment, use...) to check the system's conformity and to detect its vulnerabilities, or even to propose an action plan in case of aggression. It may also focus on determining the profile of the aggressor in order to avoid new intrusions

Objectives

The objective of this module is to present the fundamental concepts related to audit and risk management and to put them into practice on real and concrete case studies.

Skills

In terms of skills, this module aims to enable students to:

- Ensure the quality and safety of a system
- Analyze and model a constrained problem

- Assess technical solutions
- Act as a good communicator in a scientific and technical environment
- Act as a responsible professional concerned with strategic issues

Knowledge

This module enables students to develop the following concepts and skills.

- **Concepts**
  - Norms, certifications and guides
  - Law and Regulation
  - Social and societal aspects
  - Audit process: rules, key points, ethics, objectives
  - Forensic
  - Policy for Governance
  - Business Continuity Plan

- **Know-How**
  - Conduct a risk analysis
  - Organize an audit
  - Assess the relevance of corrective actions
  - Integrate Security into Projects
  - Implement Intrusion Tests

Pedagogical Approach

Fundamentals are presented by operative. Practical sessions are also provided to work on real cases.