II.3519 – Risk Management and Audit

General information

Title: Risk Management and Audit
Module ID: II.3519
Module leader: Nouredine TAMANI
ECTS: 5
Average amount of work per student: from 100 to 150 hours, including 42 hours supervised
Teamwork: yes
Keywords: Cybersecurity, Audit, Risks

Presentation

This course follows the Cybersecurity module which allows students to acquire a global understanding of the systems to be secured, whether at the level of network, information system or application development. The aim here is to study how to predict the risks to the system, and how to react in the event of a compromise.

The management of a cyber crisis covers many points: definition of the actions to be taken to resolve the crisis, but also coordination of actions, and communication with the people and organizations concerned.

Risk management aims to anticipate these crises by identifying a company's points of vulnerability, assessing the risks involved, and raising staff awareness of security issues. An audit can be carried out by experts (in installation rules, deployment, use, etc.) to verify the compliance of the system and detect its vulnerabilities or even propose an action plan in the event of an attack; It may also be a question of determining the profile of the aggressor to avoid new intrusions.

Educational objectives

Specialized skills

- Solving Constraints, Multidisciplinary Scientific and Technical Problems in the Field of ICT
    - Analysis of the problem and consideration of constraints
    - Problem modeling and formal treatment
        - Accuracies of resources used at resolution
        - Search for suitable solutions
    - Solution Assessment
        - Establish complete and consistent selection criteria
        - Be creative and innovative
        - Demonstrate critical thinking skills
- Design a software or hardware technological object with safe and standardized operation
    - Ensuring the quality and safety of a system
        - Analyze the system's mode of operation as well as malfunctions
        - Model the operation and failures of a system
        - Take into account all the standards in force, particularly those related to the environment

Prerequisite

Prerequisites: Fundamentals of cybersecurity (II.2317 / II.2417).

Content/Program

Concepts

The lessons taught in this module develop the following concepts:

- Standards, Certifications & Guides
- Law and regulation
- Social and societal aspects
- Audit process: rules, key points, ethics, objectives
- Post-mortem analysis (Forensic)
- Policy for Governance
- Business Continuity Plan

Know-how

- Conduct a risk analysis
- Organize and carry out an audit
- Assess the relevance of corrective actions
- Integrating Security into Projects
- Implementation of Penetration Tests

Pedagogical methods

Learning methods

Half of the module consists of lectures/lectures by experts in the field. The rest of the module is divided between practical application exercises (capture the flag, website attack, crisis management, audit), and real case studies.

Evaluation methods

The evaluation of this module is based on:

- Group work (2 or 3 students) on a real case study, with a written report and presentation of the work to the rest of the class (40 to 60% of the module average),
- An individual evaluation in the form of a knowledge test (60 to 40% of the module average).

Language of work

- English.
- Written presentations and reports may be made in English or French.
- The knowledge test is in English.

Bibliography, Webography, Other sources

- Course material on Moodle: https://educ.isep.fr/moodle/course/view.php?id=409