ESIROI
ÉCOLE D'INGÉNIEURS
UNIVERSITÉ DE LA RÉUNION

DEPARTMENT : *IT*
SEMESTER : *S8*

IDENTIFICATION

Course code :	ESI-SPI-CI-IN4-S8-UE4-EC3
ECTS :	1

DURATION

Lectures :	4
Tutorial classes :	12
Labs :	4
Total :	20

Project :
Personnal work :

ASSESSMENT

Continuous assessments and evaluated practical work.

TEACHING MATERIALS

Slides, directed work sheets and practical work sheets.

LANGUAGE

English

CONTACT

Tahiry RAZAFINDRALAMBO
tahiry.razafindralambo@univ-reunion.fr

Modifié le : 14 juillet 2026

UE : UE8-CYBER

COURSE : Cybersecurity : Risks, Incidents and Compliance

SCOPE OF THE COURSE

OBJECTIVES

Master the risk management, incident response and regulatory compliance approaches for an information system. Through a methodological and practical approach, students will learn to identify and qualify cyber risks, manage security incident response, and implement the requirements of current standards and regulations (GDPR, NIS2, ISO 27001).

COMPETENCE AND SKILLS

- Conduct a comprehensive risk analysis using a recognized methodology (EBIOS Risk Manager, ISO 27005) and applicable regulatory framework
- Design and implement data, network and cloud protection mechanisms in line with identified security requirements
- Define and apply an Information System Security Policy (ISSP) tailored to the organization's risks and constraints
- Manage the detection, analysis and response to a security incident using correlation tools (SIEM) and formalized procedures
- Identify legal and regulatory obligations (GDPR, NIS2, LPM) and derive the necessary compliance measures
- Draft technical and organizational documents (ISSP, incident response plan, risk analysis report) in French and English

PROGRAM

- **Introduction to cyber risk management :** fundamental concepts (threat, vulnerability, impact, likelihood), risk lifecycle, relationship between risk and security policy
- **Risk analysis methodologies :** EBIOS Risk Manager (ANSSI), ISO/IEC 27005, comparison with MEHARI and OCTAVE ; risk modeling workshops
- **Information System Security Policy (ISSP) :** development, governance, monitoring indicators, integration into the company's strategy
- **Regulatory and normative framework :** GDPR (obligations, DPO role, breach notifications), NIS2 directive, Military Programming Law (LPM), ISO/IEC 27001 and 27002
- **Security incident management :** incident lifecycle (detection, containment, eradication, recovery), response procedures, role of SOC and CERT
- **Business continuity and resilience :** Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), crisis exercises (*tabletop exercises*)
- **Audit and compliance :** internal security audit, ANSSI frameworks (SecNumCloud, security visa), implementation of an ISMS according to ISO 27001
- **Deliverables drafting :** risk analysis report, ISSP, CNIL/ANSSI incident notification form, risk treatment plan

BIBLIOGRAPHY

- Laurent Bloch & Christophe Wolfhugel - *Sécurité informatique — Principes et méthodes* - Eyrolles, 3rd ed., 2013

— Solange Ghernaouti - *Sécurité informatique et réseaux* - Dunod Editions
— Alexandre Fernandez-Toro - *Management de la sécurité de l'information — Implémentation ISO 27001* - Eyrolles, 2012
— ANSSI - *La méthode EBIOS Risk Manager* : `https://www.ssi.gouv.fr/guide/ebios-risk-manager/`
— ANSSI - *Référentiel d'exigences pour les OIV/OSE* : `https://www.ssi.gouv.fr`
— ISO/IEC 27001 :2022 - *Information security management systems*
— ISO/IEC 27005 :2022 - *Information security risk management*
— CNIL - *RGPD Guide for Developers and DPOs* : `https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on`
— NIST SP 800-61 - *Computer Security Incident Handling Guide* : `https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final`
— MITRE ATT&CK - Tactics and techniques matrix : `https://attack.mitre.org`

REQUIREMENTS

— **SEC502 - Cybersecurity : Principles, Practices and Threats :** CIA model, threat classification, introduction to security policies
— **SEC602 - Cryptography and Applications :** encryption, PKI, TLS/SSL — foundations of data protection mechanisms required by standards
— **SEC701 - Secure Architecture and Infrastructure :** design of secure architectures, firewalls, DMZ — technical context for risk analysis
— **SEC702 - Cybersecurity : Offensive Security Methodologies :** knowledge of attack techniques and vulnerabilities — essential for assessing risk likelihood
— **SEC801 - Exfiltration, Evasion and Malware :** malware analysis, IoC, evasion techniques — necessary for qualifying and handling security incidents
— **SYSRES 501 - Principles of Networks and IoT :** network protocols, addressing — basis for understanding system perimeters and mapping
— **Expected cross-disciplinary skills :**

  — Ability to draft structured technical and organizational documents
  — Reading and understanding standards and regulatory texts in French and English
  — Analytical and synthesis skills for risk modeling
  — Project management and teamwork skills