



European Funds
for Social Development



Republic
of Poland

Co-funded by the
European Union



MODULE DESCRIPTION CARD – SYLLABUS

This module is a part of the Intensive International Education Programs in the field of Cybersecurity organised at Poznan University of Technology as part of the „IMPACT – Innowacyjne Międzynarodowe Programy w AI, Cyberbezpieczeństwie i Teleinformatyce” project implemented SPINAKER Program of the National Agency for Academic Exchange, financed by the European Social Development Fund 2021–2027 (ESDF).

| Module name: | Number of hours: | Lecturer: |
|-------------------------------------|------------------|-------------------------|
| Risk Management and Security Policy | 10 | Prof. Mariusz Głąbowski |

Module Descriptions:

This module provides students with a comprehensive overview of organisational risk management and the development of effective security policies. It reflects modern approaches used in cybersecurity, enterprise governance, and regulatory compliance. Students learn how to identify and value assets, perform structured risk assessments, analyse threats and vulnerabilities, select mitigation measures, and design security policies aligned with recognised frameworks and legal requirements.

The module covers the full lifecycle of risk management—from asset discovery and threat modelling to evaluation, mitigation, monitoring, and continuous improvement. Students also explore the connection between security policies, organisational culture, awareness programs, and regulatory expectations. Real-world examples illustrate how risk-based decision-making strengthens resilience and improves compliance posture.

Purpose of the support under Module:

The module supports the strategic goals of the IMPACT program by equipping international students with competencies essential for cybersecurity governance and risk-informed decision-making. The specific objectives include:

- Understanding major risk management frameworks (ISO 31000, ISO/IEC 27005, NIST RMF).
- Learning structured approaches to risk identification, assessment, and evaluation.
- Acquiring skills in asset valuation, threat modelling, and risk analysis.
- Designing risk mitigation strategies tailored to organisational context.
- Understanding principles for developing effective security policies and governance documents.
- Learning how to implement, enforce, and monitor security policies.
- Recognising continuous-improvement mechanisms through metrics, KRIs/KPIs, and monitoring tools.
- Understanding regulatory compliance requirements and audit considerations (GDPR, NIS2, sectoral regulations).

Method of support under Module:



POZNAN UNIVERSITY OF TECHNOLOGY



European Funds
for Social Development



Republic
of Poland

Co-funded by the
European Union



Support within the module is provided with the participation of the instructor and divided into the following elements:

- 6-week self-study program using teaching materials provided by the instructor on the e-learning platform;
- 6 weeks of support from the instructor in the form of online consultations using tools that enable meetings to be held;
- a test to verify the acquisition of competences.

Module-related learning outcomes:

Knowledge:

Upon successful completion, the student:

1. Understands the foundations of formal risk management frameworks and standards.
2. Knows methodologies for risk assessment, including qualitative, quantitative, and hybrid approaches.
3. Understands asset identification, classification, and valuation principles.
4. Knows threat modelling techniques such as STRIDE, attack trees, and scenario-based models.
5. Understands methods of likelihood/impact analysis, risk matrices, and evaluation criteria.
6. Knows risk treatment options: mitigation, transfer, avoidance, and acceptance.
7. Understands how security policies support governance, compliance, and risk reduction.
8. Knows policy development lifecycle and key components of effective security policies.
9. Understands monitoring, measurement, and continuous improvement mechanisms.
10. Knows regulatory compliance requirements and the role of audits in governance frameworks.

Skills:

The student:

1. Can identify assets, assess their value, and document dependencies.
2. Can apply structured frameworks to evaluate threats, vulnerabilities, and risks.
3. Can construct risk matrices and perform basic quantitative or qualitative risk scoring.
4. Can select appropriate risk treatment strategies and justify mitigation decisions.
5. Can develop or review security policies aligned with organisational goals and regulatory needs.
6. Can design awareness programs that support policy enforcement and behavioural change.
7. Can propose meaningful metrics for monitoring and improving organisational security.
8. Can prepare for basic compliance assessments and understand audit expectations..

Social competences:



POZNAN UNIVERSITY OF TECHNOLOGY



European Funds
for Social Development



Republic
of Poland

Co-funded by the
European Union



The student:

1. Understands the importance of risk-based thinking in organisational decision-making.
 2. Recognises the role of security culture and human factors in policy effectiveness.
 3. Demonstrates responsibility and ethical awareness when evaluating risk and compliance issues.
 4. Appreciates the need for interdisciplinary collaboration in risk management and governance.
-

Criteria for verifying learning outcomes

Learning outcomes of the course are verified via an assessment test.

Method of verification/validation of learning outcomes

The verification of the learning outcomes is based on answers to the questions in the test.
The test is passed if the student answers correctly at least 50% of the questions.

Workload

25 h (including work with teaching materials provided by the lecturer, consultation, and the student's own work) – 1 ECTS point

Level of the European Qualifications Framework



POZNAN UNIVERSITY OF TECHNOLOGY