COURSE OUTLINE

SCHOOL	Sciences and Engineering		
ACADEMIC UNIT	Computer Science		
LEVEL OF STUDIES	1st Cycle		
COURSE CODE	COMP-230	**SEMESTER**	Spring
COURSE TITLE	Cybersecurity Governance		

INDEPENDENT TEACHING ACTIVITIES *if credits are awarded for separate components of the course, e.g. lectures, laboratory exercises, etc. If the credits are awarded for the whole of the course, give the weekly teaching hours and the total credits*	**WEEKLY TEACHING HOURS**	**CREDITS**
	2.5	6
Add rows if necessary. The organisation of teaching and the teaching methods used are described in detail at (d).		

COURSE TYPE *general background, special background, specialised general knowledge, skills development*	Specialization
PREREQUISITE COURSES:	Sophomore Standing
LANGUAGE OF INSTRUCTION and EXAMINATIONS:	English
IS THE COURSE OFFERED TO ERASMUS STUDENTS	
COURSE WEBSITE (URL)	

LEARNING OUTCOMES

Learning outcomes

The course learning outcomes, specific knowledge, skills and competences of an appropriate level, which the students will acquire with the successful completion of the course are described.

Consult Appendix A

- *Description of the level of learning outcomes for each qualifications cycle, according to the Qualifications Framework of the European Higher Education Area*
- *Descriptors for Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Appendix B*
- *Guidelines for writing Learning Outcomes*

After completion of the course students are expected to be able to:

- define cybersecurity governance and articulate its strategic importance
- design and implement cybersecurity governance documentation
- analyze and apply the principles and legal obligations of GDPR
- compare and contrast GDPR with related data protection regulations

- conduct a cybersecurity risk assessment within a governance framework
- apply cybersecurity governance frameworks to real-world organizational contexts
- evaluate the maturity and effectiveness of cybersecurity governance programs
- develop a comprehensive cybersecurity governance and compliance plan

LEARNING OUTCOMES

Learning outcomes

The course learning outcomes, specific knowledge, skills and competences of an appropriate level, which the students will acquire with the successful completion of the course are described.

Consult Appendix A

- *Description of the level of learning outcomes for each qualifications cycle, according to the Qualifications Framework of the European Higher Education Area*
- *Descriptors for Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Appendix B*
- *Guidelines for writing Learning Outcomes*

After completion of the course students are expected to be able to:

- define cybersecurity governance and articulate its strategic importance
- design and implement cybersecurity governance documentation
- analyze and apply the principles and legal obligations of GDPR
- compare and contrast GDPR with related data protection regulations
- conduct a cybersecurity risk assessment within a governance framework
- apply cybersecurity governance frameworks to real-world organizational contexts
- evaluate the maturity and effectiveness of cybersecurity governance programs
- develop a comprehensive cybersecurity governance and compliance plan

General Competences

Taking into consideration the general competences that the degree-holder must acquire (as these appear in the Diploma Supplement and appear below), at which of the following does the course aim?

Search for, analysis and synthesis of data and information, with the use of the necessary technology
Adapting to new situations
Decision-making
Working independently
Team work
Working in an international environment
Working in an interdisciplinary environment
Production of new research ideas

Project planning and management
Respect for difference and multiculturalism
Respect for the natural environment
Showing social, professional and ethical responsibility and sensitivity to gender issues
Criticism and self-criticism
Production of free, creative and inductive thinking
……
Others…
…….

- *Search for, analysis and synthesis of data and information, with the use of the necessary technology*
- *Adapting to new situations*
- *Decision-making*
- *Team work*
- *Working in an interdisciplinary environment*
- *Project planning and management*

SYLLABUS

1. Introduction to Cybersecurity Governance
    a. Overview of governance principles, strategic alignment, and its role in cybersecurity management
2. Roles, Responsibilities, and Organizational Structures
    a. Governance roles including board oversight, CISO, DPO, and security committees
3. Security Policies, Standards, and Procedures
    a. Policy frameworks, development lifecycle, enforcement mechanisms, and policy governance
4. Cybersecurity Governance Frameworks
    a. NIST CSF, ISO/IEC 27001, COBIT 2019, and CIS Controls
    b. Adoption and implementation
5. Cyber Risk Management and Decision-Making
    a. Risk assessment methodologies
    b. Threat modeling
    c. Risk tolerance
    d. Mitigation strategies
6. Legal and Regulatory Foundations of Cybersecurity
    a. Overview of global regulations: GDPR, HIPAA, SOX, FISMA, PCI-DSS, and emerging legislation.
7. Data Protection Frameworks
    a. GDPR: Principles, Roles, and Compliance Requirements: Lawfulness of processing, data subject rights, breach notification, DPO duties, and accountability.
    b. Comparison of GDPR with CCPA, HIPAA, ISO/IEC 27701, PIPEDA, and Privacy by Design
8. Compliance, Monitoring, and Auditing
    a. Compliance lifecycle, audit practices, control testing, regulatory reporting, and remediation.
9. Measuring and Improving Governance Maturity
    a. KPIs and KRIs
    b. COBIT maturity levels
    c. Performance reviews

10. Case Studies
    a. Analysis of major governance incidents (e.g., Equifax, SolarWinds)

TEACHING and LEARNING METHODS - EVALUATION

<table>
<tr><td><b>DELIVERY</b>
<i>Face-to-face, Distance learning, etc.</i></td><td>Face-to-face</td></tr>
<tr><td><b>USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY</b>
<i>Use of ICT in teaching, laboratory education, communication with students</i></td><td><i>Use of ICT in teaching / Χρήση ΤΠΕ</i>
<i>Communication with students / Επικοινωνία με Φοιτητές</i></td></tr>
<tr><td><b>TEACHING METHODS</b>
<i>The manner and methods of teaching are described in detail.</i>
<i>Lectures, seminars, laboratory practice, fieldwork, study and analysis of bibliography, tutorials, placements, clinical practice, art workshop, interactive teaching, educational visits, project, essay writing, artistic creativity, etc.</i>
<i>The student's study hours for each learning activity are given as well as the hours of non-directed study according to the principles of the ECTS</i></td><td>
<table>
<tr><th><i>Activity</i></th><th><i>Semester workload</i></th></tr>
<tr><td>Lectures</td><td>35</td></tr>
<tr><td>Preparation, assignments</td><td>53</td></tr>
<tr><td>Project</td><td>40</td></tr>
<tr><td>Exam preparation</td><td>20</td></tr>
<tr><td>Final Exam</td><td>2</td></tr>
<tr><td>Course total</td><td><b><i>150</i></b></td></tr>
</table>
</td></tr>
<tr><td><b>STUDENT PERFORMANCE EVALUATION</b>
<i>Description of the evaluation procedure</i>
<i>Language of evaluation, methods of evaluation, summative or conclusive, multiple choice questionnaires, short-answer questions, open-ended questions, problem solving, written work, essay/report, oral examination, public presentation, laboratory work, clinical examination of patient, art interpretation, other</i>
<i>Specifically-defined evaluation criteria are given, and if and where they are accessible to students.</i></td><td>Homework, Project, Mid-Term, Final Exam</td></tr>
</table>

ATTACHED BIBLIOGRAPHY

Assessment Methods:

Assignments, Project, Mid-Term, Final Exam

Required Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Information security governance: A practical development and implementation approach (2nd ed.)	Krag Brotby	Wiley	2024	9781118482414

Recommended Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Managing information security risks: The OCTAVE approach	Alberts Christopher and Dorofee Audrey	Addison-Wesley Professional	2002	9780321118868
The EU General Data Protection Regulation (GDPR): A practical guide (2nd ed.)	Voigt Paul and von dem Bussche Axel	Springer-Cham	2024	9783031623271
Security Risk Management: Building an Information Security Risk Management Program from the	Wheeler Evan	Syngress	2014	9780128006941

Ground Up (2nd ed.)				