Cyber Security and Cyber Resilience

26FS

Programme	MSc in Business Information Systems
Degree	Master
ECTS	6
Module type	elective module
Module coordinator	Prof. Dr. Petra Asprion
Compulsory attendance	Participation is expected.
Leading principle / Short description	As threats to cyber security become increasingly ominous, sophisticated, and unpredictable, CEOs, CIOs and other decision makers must address related risks. In addition, large organizations must manage complex networks of service providers and many of whom have access to customers, sensitive data, and critical technology. Under these circumstances, many organizations struggle to maintain the continuous vigilance and end-to-end visibility across the entire service delivery chain that is essential to a viable cybersecurity strategy and the resulting operationalization. In this course, we derive key challenges of cybersecurity and how effectively address them by adopting relevant frameworks, best practices as well as governance mechanisms claimed as "cyber resilience". Where appropriate, we also touch on areas of information or information security. Special emphasis will be placed on ´Data Privacy and Protection´ and ´Technical Insights´. The course does not focus on very technical aspects but on the systemic, governance and management level in dealing with cyber risks.
Module content	**Part I – Organizational Perspectives** 1. Cyber risk landscape and uncertainties 2. Strategic relevance and CERT insights 3. Governance, culture, and leadership for resilience 4. Frameworks and standards (NIST, ISO, COBIT, etc.) **Part II – Technical Perspectives** 1. Modern threat landscape (APT, ransomware, cloud/IoT, AI) 2. Vulnerabilities, secure coding, and DevSecOps 3. Detection and response (SIEM, SOAR, threat intelligence) 4. Protective architectures (zero trust, encryption, IAM) 5. Resilience engineering (redundancy, recovery, cyber ranges)
Competencies to be achieved	This course provides participants with a deep understanding of current cyber risks and their impact on enterprises and decision-makers. They will learn key mechanisms to assess, protect, respond, and mitigate risks—while addressing regulatory demands, global vs. local requirements, and modern governance models. The focus is on practical application: conducting awareness assessments, applying cybersecurity concepts in real-world contexts, and deriving prioritized recommendations. Communication skills are also strengthened through discussions on resilience strategies (e.g., NIST, ISO 27K), relevant metrics, and critical debates on topics such as ethical hacking. The course combines self-directed learning with best practices, reference models, and hands-on exercises—including practical experience.
Prerequisites	Participants should have knowledge of fundamental IT management and governance mechanisms
Teaching and learning methods	**Lecture** Discussion | Presentation | Assignment | Case study | Simulation **Guided Self-Study Individual work** Individual work | Working with a partner | Group work
Literature	provided on Moodle
Remarks	In this module, you will learn how to tackle complex cyber threats by combining organizational strategies with technical defenses. Through case studies and simulations, you will gain practical experience and develop the skills needed to strengthen resilience and shape your career as a future security expert.

Grading

Grade 1-6 (half grades)

Assessment

Assignment 50%	
Oral / Written	written
Timeframe	during the semester
Grading Scale	Grades 1-6 (half grades) - at least grade 3.5
Exam 50%	
Duration (min)	90
Timeframe	During the eam period at the end of the semester
Grading Scale	Grade 1-6 (half grades) - at least grade 3.5

Module details

26FS.Cyber Security and Cyber Resilience - Wed - Olten	
Time	1:15 PM - 5:00 PM
Periodicity	Weekly
Lecturers	Prof. Dr. Petra Asprion
Number	3-26FS.W-M-BIS-E CSCR.EN