Course Title	Cybersecurity Risk Analysis and Management				
Course Code	CYS675				
Course Type	Optional				
Level	Master (2nd cycle)				
Year / Semester	2nd Year/3rd Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	This course introduces the fundamental concepts of cybersecurity risk analysis and management, as well as its position as the foundation for cybersecurity protective mechanisms. It covers a wide range of principles and processes related to risk management, and sets the scene for the development of comprehensive cybersecurity controls to protect an organizations assets according to the risk appetite of senior management.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Describe the underlying principles of risk analysis and management and the purpose and benefits behind such activities • Explain the terms used, such as risk, analysis, management, vulnerability, threats, actors, impact, risk matrix, etc. • Recognise the difference between vulnerabilities and threats. • Classify and describe a number of different risk assessment/management methodologies. • Classify and describe different assets and their values (including tangible and intangible assets). • Identify and explain various threat sources and the impacts that their materialization may manifest. • Describe the risk management process, as it pertains to the protection of assets. • Evaluate and select appropriate risk treatment options according to the combination of impacts and probabilities that the risk analysis has produced.				
Prerequisites	None	Co-requisites	CYS600		
Course Content	Introduction: Definition of cybersecurity risk and associated terminology, the position of risk analysis and management in relation to the other components of a cybersecurity programme.				

	Principles: Assets, vulnerabilities, threats, threat actors, likelihood. Management of risks compared to simple acceptance. Risk treatment options: avoidance, mitigation, transfer, acceptance. Assets: Tangible and intangible assets in the cyber world (hardware / software / data, classification, criticality based on the importance and value to organization (not just monetary), dependencies, potential for critical national infrastructure. Vulnerabilities: Sources of cyber vulnerability, complexity of modern software, attack surface of modern systems, development of software for functionality and not with security considerations, existing known and zero-day system vulnerabilities, vulnerability databases and open information. Threats: Cyber threat categorization, sources, motivation, type, technical vs. non technical (e.g. attacks to cooling systems to disrupt cyber systems), threat actors, exploitation of cyber vulnerabilities leading to impact and associated likelihood. Risk analysis: Risk as a combination of possible impact of a threat exploiting a vulnerability and the probability of such an impact occurring, evaluation of cyber risks, categorization, qualitative and quantitative risk analysis, pre-requisites for meaningful quantitative cyber risk assessment, methodologies, risk register. Risk management: Risk evaluation and associated selection of risk treatment options, effects and selection of risk avoidance, mitigation, transfer, acceptance (or a combination thereof), risk management as an iterative process, risk profile stemming from modifications in an organisation's environment, building an organisation's cybersecurity control environment from the results of risk analysis, introduction to basic cybersecurity controls. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practical uses challenges of risk analysis and management in real environments.
Teaching Methodology	E-Learning
Bibliography	*"Effective Cybersecurity: A Guide to Using Best Practices and Standards, by William Stallings* *"Cyber-Risk Management" by Atle Refsdal, Bjørnar Solhaug, Ketil Stølen* *"Security Risk Management: Building an Information Security Risk Management Program from the Ground Up"*, by Evan Wheeler

	"How to Measure Anything in Cybersecurity Risk", by Douglas W. Hubbard and Richard Seiersen *"The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)"*, by Anne Kohnke and Dan Shoemaker
Assessment	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English