

Course Title	Cybersecurity Policy, Governance, Law and Compliance				
Course Code	CYS630				
Course Type	Compulsory				
Level	Master (2 <sup>nd</sup> cycle)				
Year / Semester	1 <sup>st</sup> Year/2 <sup>nd</sup> Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	This course provides an overview of the broad and constantly emerging field of cybersecurity policy, governance, law and compliance. The importance of the role of security policy is discussed.				
Learning Outcomes	<p>Upon successful completion of this course, students should be able to:</p> <ul style="list-style-type: none"> <li>• State and identify concepts relating to organizational cybersecurity policy, governance mechanisms, applicable legislation and compliance requirements for information security.</li> <li>• State and interpret the different components of a comprehensive organizational cybersecurity policy.</li> <li>• State and interpret the role of security policy within an organization and its position with relation to other controls within a comprehensive cybersecurity environment.</li> <li>• Describe the role of corporate governance with regards to cybersecurity, and the business reasons for implementing a cybersecurity function.</li> <li>• Recognize and explain major applicable legislation and regulatory framework (local, European, international).</li> <li>• Define, explain and exemplify compliance requirements in relation to cybersecurity, information security, data protection (privacy, anonymity) and critical information infrastructure protection.</li> </ul>				
Prerequisites	None		Co-requisites	CYS600	

Course Content	<p><u>Introduction:</u> Concepts of cybersecurity, its relationship with network and information security, cybercrime, cyberdefence, and related definitions. Concepts of policy, governance, related law and compliance, and the relationships between them.</p> <p><u>Principles:</u> Information security components and concepts, confidentiality, integrity, availability.</p> <p><u>Policy:</u> definition, role of policy in an organization, statement of management purpose and organizational objectives, description of organizational approach, standards, baselines, guidelines, procedures.</p> <p><u>Governance:</u> Role of cybersecurity and information security in the organization, levels of responsibility, the different personnel roles: information owner, information custodian, administrator, solution provider, change control, human resources, user. Certification and accreditation.</p> <p><u>Law:</u> Relevant laws and legal/regulatory frameworks on the national, European and international level. Different types of law related to cyberattacks – computer as the means, computer as a victim. Problems of jurisdiction, borderless nature of cybercrime, relevance and importance of data protection and privacy, investigations.</p> <p><u>IT and Law:</u> Introduction, Terminology, and the Nature of Cyberspace and Threats. Cyber-regulation and cyber-regulatory theory. Cyberproperty and Intellectual Property. Cyber-rights, Speech Harm, Crime and Control. Roles of International Law, the State, and the Private Sector in Cyberspace. Authentication and Identity Management. Speech, Privacy and Anonymity in Cyberspace. Trust.</p> <p><u>Compliance:</u> Reasons for specific cybersecurity legislation beyond cybercrime, compliance requirements, self-assessment, auditing principles, audit process.</p> <p>Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on reasons behind and expected benefits of compliance requirements and on recent/future developments.</p>
Teaching Methodology	E-Learning
Bibliography	<p><i>“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”</i>, by Evan Wheeler</p> <p><i>“Information Security Governance: A Practical Development and Implementation Approach”</i>, by Krag Brotby</p> <p><i>“Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats”</i>, by Scott E. Donaldson</p>

	<i>“Cyber Security and IT Infrastructure Protection”</i> , by John R. Vacca	
Assessment	Examinations	50%
	Assignments/On-going evaluation	50%
		100%
Language	English	