

Course Title	Cybersecurity Architecture and Operations				
Course Code	CYS660				
Course Type	Compulsory				
Level	Master (2 nd cycle)				
Year / Semester	1 st Year / 2 nd Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	3 Hours	Laboratories / week	None
Course Purpose and Objectives	<p>This course introduces the fundamental security principles of confidentiality, integrity, availability, as well as related security services such as accountability, non-repudiation, authentication, etc. The whole operational environment is described, with reference to ongoing security processes such as user provisioning, vulnerability management, penetration testing, exercising, change management, incident response, risk assessment and others. The five phases of cybersecurity are discussed here – Identify, Protect, Detect, Respond, Recover.</p>				
Learning Outcomes	<p>Upon successful completion of this course students should be able to:</p> <ul style="list-style-type: none"> • Identify the various components of a comprehensive cybersecurity architecture within an organization. • Describe the underlying principles of defense in depth and control objectives associated with the outputs of a risk assessment. • Describe and classify controls that meet specific control objectives and to treat identified risks. • Explain in detail the basic security principles of confidentiality, integrity and availability, as well as related security services such as accountability, non-repudiation, authentication, etc. • Describe the five phases of cybersecurity operations: Identify, Protect, Detect, Respond, Recover. • Evaluate available controls and the degree to which they mitigate risks. • Select and propose additional controls as appropriate. • Describe and evaluate the processes of vulnerability management, penetration testing, exercising, change management, incident response, and others. 				

	<ul style="list-style-type: none"> • Recognise and explain the differences between normal and emergency operations. • Classify and describe a number of different effects of main cybersecurity controls on the operational environment, e.g. access control. • Evaluate and select appropriate architectural and operational options according to the organizational risk environment. 		
Prerequisites	None	Co-requisites	None
Course Content	<p><u>Introduction:</u> Definition of security objectives: confidentiality, integrity, availability, accountability non-repudiation, authentication.</p> <p><u>Processes:</u> User provisioning, access control, vulnerability management, penetration testing, exercising, change management, incident response, others.</p> <p><u>Phases:</u> Phases of cybersecurity operations, in relation to the before and after of an incident: Identify, Protect, Detect, Respond, Recover.</p> <p><u>Identify:</u> Identification of organizational assets, threats, vulnerabilities and risks (details in risk assessment course), vulnerability management (open databases, CVE, etc.) as an essential process.</p> <p><u>Protect:</u> Selection and evaluation of controls to meet control objectives and risks identified, application and monitoring of controls, control lists (ISO 27002, COBIT 5, SANS 20 Critical Controls, Australia DSD Top Mitigations, etc), defense-in-depth considerations, penetration testing, BCP and DRP testing, system hardening.</p> <p><u>Detect:</u> Detection of cybersecurity incidents as they occur, evaluation of impacts, log analysis, IDS/IPS, attack vector analysis, SIEM (security incident and event management), indicators of compromise (IOC).</p> <p><u>Respond:</u> Incident triage and response, CERT/CSIRTs, triggering and implementation of business continuity and disaster recovery plans, corrective controls.</p> <p><u>Recover:</u> Orderly and planned return to prior operational status and capabilities, lessons learned, evaluation of corrective controls and supporting processes.</p> <p>Specific cybersecurity operations topics: Database security, secure software development, mechanisms for ensuring the security of</p>		

	<p>information at rest, in transit, and during processing, side-channel considerations.</p> <p>Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practicalities of cybersecurity operations in real environments.</p>						
Teaching Methodology	Face – to – face						
Bibliography	<p><i>“Cybersecurity Operations Handbook”</i>, by John Rittinghouse and William M. Hancock</p> <p><i>“Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”</i>, by Thomas A. Johnson (Editor)</p> <p><i>“The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”</i>, by Anne Kohnke and Dan Shoemaker</p> <p>ISO 27002 - <i>Information technology – Security techniques – Code of practice for information security management</i></p> <p>COBIT 5</p> <p>SANS 20 Critical Controls</p> <p>Australia Defense Signals Directorate Top Mitigations</p> <p>IEEE Journals and Magazines</p>						
Assessment	<table border="1"> <tr> <td>Examinations</td> <td>60%</td> </tr> <tr> <td>Assignment(s)</td> <td>40%</td> </tr> <tr> <td></td> <td>100%</td> </tr> </table>	Examinations	60%	Assignment(s)	40%		100%
Examinations	60%						
Assignment(s)	40%						
	100%						
Language	English						