Faculty: Information Technology	
Department: Cybersecurity	**Program: Master**
Academic year:	**Semester:**

Course Plan

First: Course Information

Course No.: 1506723	*Course Title:* Cybersecurity Risk Management	*Credit Hours: 3*	*Theoretical: 3*	*Practical: 0*
Prerequisite No. and Title:	*Section No.:*	*Lecture Time:*		
Level in JNQF	*9*			
Type Of Course:	□ *Obligatory University Requirement* □ *Obligatory Faculty Requirement* □ *Obligatory Specialization Requirement* □ *Ancillary course*	□ *Elective University Requirement* □ *Elective Faculty Requirement* ■ *Elective Specialization Requirement*		
Type of Learning:	□ *Face-to-Face Learning* ■ *Blended Learning (2 Face-to-Face + 1 Asynchronous)* □ *Online Learning (2 Synchronous+ 1 Asynchronous)*			

Second: Instructor's Information

Course Coordinator:					
Name:	*Academic Rank:*				
Office Number:	*Extension Number:*	*Email:*			
Course Instructor:					
Name:	*Academic Rank:*				
Office Number:	*Extension Number:*	*Email:*			
Office Hours:	*Sunday*	*Monday*	*Tuesday*	*Wednesday*	*Thursday*

Third: Course Description

This course covers the professional practice of cyber security risk management considered from the perspective of enterprise governance. It encompasses cyber security risk identification, classification, measurement, remediation, monitoring and reporting. Concepts are explained with examples and illustrations to accelerate the learning process.

Fourth: Course Objectives

1. Introducing the student to the concepts, theories, principles and practices of Risk Management.
2. Developing the student’s ability to deal with Risk Management in Cyber Security.
3. Analyze the cyber security threats, vulnerabilities and risks faced by an organization
4. Assess the cyber security posture of an organization and recommend and implement appropriate solutions
5. Test, monitor and continually improve the effectiveness of an organization's cyber security defense mechanisms.
6. Formulate cyber security and data protection policies and procedures for an organization.

Fifth: Learning Outcomes

Level descriptor according to (JNQF)	*CILOs Code*	*CILOs* If any CLO will not be assessed in the course, mark NA.	*Associated PILOs Code* *Choose one PILO for each CILO**	*Assessment method* *Choose at least two methods*
Knowledge	**K1**	Provide the students with the basic and advanced practice of Risk Management in Cyber Security	**PK1**	• Mid-term Exam • Final Exam • Research
	K2	Describe the underlying principles of risk analysis and management	**PK2**	• Mid-term Exam • Final Exam • Research
	K3	Recognize the difference between vulnerabilities and threats	**PK3**	• Mid-term Exam • Final Exam • Research
	K4	Classify and describe a number of different risk assessment/management methodologies	**PK4**	• Mid-term Exam • Final Exam • Research
Skills	**S1**	Identify and explain various threat sources and the impacts that their materialization may manifest	**PS1**	• Mid-term Exam • Final Exam • Research
	S2	Describe the risk management process, as it pertains to the protection of assets	**PS2**	• Mid-term Exam • Final Exam • Research
	S3	Evaluate and select appropriate risk treatment options according to the combination of impacts and probabilities that the risk analysis has produced.	**PS3**	• Mid-term Exam • Final Exam • Research
	S4	Conduct independent research to better comprehend a certain topic or stay current with field developments.	**PS4**	• Mid-term Exam • Final Exam

				• Research
Competencies	**C1**	Utilize different techniques for dealing with risk management in cyber security.	**PC3**	• Mid-term Exam • Final Exam • Research
	C2	Develop effective communication skills with the students in the proper way to deliver the required skills and providing them with knowledge about risk management	**PC4**	• Mid-term Exam • Final Exam • Research

*CILOs: Course Intended Learning Outcomes; PILOs: Program Intended Learning Outcomes; For each CILO, the PILO could be the same or different.

Sixth: Learning Resources

Main Reference:	**Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework**		
Author: Brian Haugli	***Issue No.:1th***	*Print:*	***Publication Year:2021***
Additional Sources &Websites:	• Research Papers • How to Measure Anything in Cybersecurity Risk v2, Richard Seiersen, 1st Edition 2023, ISBN-10: 1119892309 | ISBN-13: 978-1119892304 • Fundamentals of Adopting the NIST Cybersecurity Framework, David Moskowitz, Kindle Edition 2022, ISBN-13: 978-0117093706 • An Introduction to Computer Security: the NIST Handbook, http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf Access on June 29, 2022 • Cybersecurity, http://www.windowsecurity.com/whitepaper/ Access on June 29, 2022		
Teaching Type:	□ ***Classroom*** □ ***Laboratory*** □ ***Workshop*** ■ ***MS Teams*** ■ ***Moodle***		

Seventh: Course Structure

Lecture Date	**Course Intended Teaching Outcomes (CILOs)**	**Topics**	**Teaching Procedures***	**Teaching Methods****	**References*****
Week 1	C2, K1	An Overview of Cybersecurity Risk Management	Face-to-Face	Lecturing	Textbook-ch1
Week 2	C2, K1	Asset Management, Governance, Risk Assessment and Management	Face-to-Face	Lecturing, Assignments	Textbook-ch1, Research Papers
Week 3	S1, K2, K3, K4	User and Network Infrastructure Planning and Management	Asynchronous	Assignment, videos, Quiz	Textbook-ch2
Week 4	S1, K2, K3, K4	Identity Management, Authentication, and Access Control, Awareness and Training	Face-to-Face	Lecturing, Assignments	Textbook-ch2
Week 5	S1, K2, K3, K4	Data Security, Information	Face-to-Face	Lecturing, Assignments	Textbook-ch2

		Protection Processes and Procedures, Word about Patch Management, Maintenance, Protective Technology			
Week 6	S2, K2, K3, K4	Tools and Techniques for Detecting Cyber Incidents	Asynchronous	Assignment, videos, Quiz	Textbook-ch3
Week 7	S2, K2, K3, K4	Anomalies and Events, Word about Antivirus Software, Continuous Monitoring, Detection Processes	Face-to-Face	Lecturing, Assignments	Textbook-ch3, Research Papers
Midterm Exam					
Week 8	S3, K2, K3, K4	Developing a Continuity of Operations Plan	Face-to-Face	Lecturing, Assignments	Textbook-ch4
Week 9	S3, K2, K3, K4	Response, Analysis,	Asynchronous	Assignment, videos	Textbook-ch4
Week 10	S1, K2, K3, K4	Mitigation, Recover	Face-to-Face	Lecturing	Textbook-ch4, Research Papers
Week 11	S2, K2, K3, K4	Supply Chain Risk Management	Face-to-Face	Lecturing, Assignments	Textbook-ch5
Week 12	C1, C2, S3, S4, K1	Software Bill of Materials, NIST Revised Framework Incorporates Major Supply Chain Category	Asynchronous	Assignment, videos, Quiz	Textbook-ch5
Week 13	C1, C2, S3, S4, K1	Manufacturing and Industrial Control Systems Security	Face-to-Face	Lecturing	Textbook-ch6, Research Papers
Week 14	C1, C2, S3, S4, K1	Essential Reading on Manufacturing and Industrial Control Security	Face-to-Face	Lecturing, Assignments	Textbook-ch6
Final Exam					

*Teaching procedures: (Face-to-Face, synchronous, asynchronous). ** Teaching methods: (Lecture, video….).
*** Reference: (Pages of the book, recorded lecture, video….)

Eighth: Assessment Methods

Methods	Online Learning	Blended Learning	Face-To-Face Learning	Specific Course Output to be assessed **If any CILO will not be assessed in the course, mark NA.									
				K1	K2	K3	K4	S1	S2	S3	S4	C1	C2
First Exam													
Second Exam													
Mid-term Exam		30			✓		✓	✓	✓	✓			✓
Participation													
Asynchronous Activities		20		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Quizzes		10		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Assignments/ Research													
Group presentation													
Final Exam		40		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Total out of 100		100											

Ninth: Course Policies

- All course policies are applied to all teaching patterns (online, blended, and face-to-face Learning) as follows:
  a. Punctuality.
  b. Participation and interaction.
  c. Attendance and exams.
- Academic integrity: (cheating and plagiarism are prohibited).

Approval	Name	Date	Signature
Head of Department			
Faculty Dean			