Course Specification

(Postgraduate)

Course Title:	Risk Management in Cybersecurity
Course Code:	CYBS60311
Program:	M.Sc. in Cybersecurity
Department:	Department of Computer Science
College:	Faculty of Computing and Information
Institution:	Al-Baha University
Version:	1
Last Revision Date:	*Pick Revision Date.*

Table of Contents

A. General information about the course: 3

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods: 4

C. Course Content: 5

D. Students Assessment Activities: 5

E. Learning Resources and Facilities: 6

F. Assessment of Course Quality: 7

G. Specification Approval Data: 7

A. General information about the course:

1. Course Identification:

1. Credit hours: (3)				
2. Course type				
A.	☐University	☐College	☒ Department	☐Track
B.	☐ Required		☒ Elective	
3. Level/year at which this course is offered: (2/5th)				
4. Course general Description:				
Risk Management in Cybersecurity is designed to equip students with the proficiency to analyze and manage cybersecurity risks effectively. This course emphasizes the relationship between security policy and risk, and explores various risk management and analysis methodologies. Students will learn to evaluate and categorize risks associated with technology, individuals, and entities, and select appropriate methodologies for cyber risk management. Key topics include the lifecycle of risk management, assessment methodologies, measuring and evaluating cyber risks, management standards, and the economics of risk mitigation. Additionally, the course covers risk policies and the impact of organizational characteristics on cyber risk analysis, concluding with effective communication strategies for cyber risks.				
5. Pre-requirements for this course (if any):				
6. Pre-requirements for this course (if any):				
7. Course Main Objective(s):				
By the end of this course, students are expected to: ☐ Understand and apply cybersecurity risk management principles. ☐ Demonstrate proficiency in risk analysis methodologies ☐ Evaluate and strategize cyber risks ☐ Integrate organizational dynamics in risk management ☐ Effectively communicate cybersecurity risks				

2. Teaching Mode: (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	26	80%
2	E-learning	7	20%
3	Hybrid		

No	Mode of Instruction	Contact Hours	Percentage
	☐ Traditional classroom ☐ E-learning		
4	Distance learning		

3. Contact Hours: (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	33
2.	Laboratory/Studio	-
3.	Field	-
4.	Tutorial	-
5.	Others (specify)	-
	Total	33

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods:

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Describe the connection between the rules for protecting an organization from cyberattacks and the potential risks and consequences of those attacks	**K1**	☐ Lectures ☐ Assignments ☐ Group Discussion	☐ Assignments ☐ Midterm Exam ☐ Final Exam
1.2	Identify and explain the main methods for assessing and analyzing cyber risks	**K2**	☐ Lectures ☐ Assignments ☐ Group Discussion	☐ Assignments ☐ Midterm Exams ☐ Final Exam
1.3	Assess and differentiate risks in diverse cyber contexts	**K3**	☐ Lectures ☐ Assignments ☐ Group Discussion	☐ Assignments ☐ Midterm Exams ☐ Final Exam
2.0	**Skills**			
2.1	Apply risk analysis methodologies to real-world scenarios	**S1**	☐ Lectures ☐ Assignments ☐ Project	☐ Quiz ☐ Midterm exam ☐ Final Exam

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
				☐ Project
2.2	Develop and implement security policies addressing identified risks	**S2**	☐ Lectures ☐ Assignments ☐ Project	☐ Quiz ☐ Midterm exam ☐ Final Exam Project
3.0	**Values, autonomy, and responsibility**			
3.1	Demonstrate Ethical Judgment and Responsibility in Cybersecurity Risk Management	**V1**	☐ Project	☐ Project evaluation form (rubric)

C. Course Content:

No	List of Topics	Contact Hours
1	Fundamentals of Risk Analysis and Management in Cybersecurity	3
2	Risk Management Lifecycle and Steps	3
3	Risk Identification, assessment and Evaluation Techniques in Cybersecurity	3
4	Techniques for Quantifying and Assessing Cybersecurity Risks	3
5	Standards and Frameworks in Cybersecurity Risk Management	3
6	Risk Management Processes Within Organizational Structures	3
7	Economic Aspects of Mitigating Cybersecurity Risks	3
8	Transference, Acceptance and Mitigation of Cyber Risks	3
9	Cyber Risks Policies for Technologies, Individuals and Entities	3
10	Influence of Organizational Traits on Cybersecurity Risk Processes	3
11	Communication of Cyber Risks	3
12	Emerging Trends and Future Challenges in Cybersecurity Risk Management	
Total		**33**

D. Students Assessment Activities:

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1	Assignments	Every 2 weeks	10%
2	Midterm exam	Week 6	20%
3	Quiz	Week 8	10%
4	Project	Week 11	10%

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
5.	Final Exam	Week 13	50%

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

E. Learning Resources and Facilities:

1. References and Learning Resources:

Essential References	M. Harkins, *Managing Risk and Information Security: Protect to Enable*. Springer Science+Business Media, 2016. C. Brumfield and B. Haugli, *Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework*. Hoboken, NJ: John Wiley & Sons, Inc, 2023.
Supportive References	*Cyber Risk Resources for Practitioners*. London: The Institute of Risk Management, 2014. *CRISC Review Manual*, 7th ed. Schaumburg, IL: ISACA, 2021.
Electronic Materials	• Access to the Saudi Digital Library (SDL). • Using the learning management system of the university – Rafid System (https://rafid.bu.edu.sa). • Saudi National Cybersecurity Authority (NCA) (https://nca.gov.sa)
Other Learning Materials	

2. Educational and Research Facilities and Equipment Required:

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	• A classroom or lecture hall with whiteboard for 25 students.
Technology equipment (Projector, smart board, software)	All students shall have • A laptop or access to a desktop computer with access to a programming development tool. • High speed Internet connection • Power outlets for student's laptop plug-in Relevant programming software for use of students.
Other equipment (Depending on the nature of the specialty)	• The laboratory should have computers with programming development tools.

F. Assessment of Course Quality:

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students - Program Leaders	Indirect
Effectiveness of students assessment	Program Leaders	Indirect
Quality of learning resources	Students	Indirect
The extent to which CLOs have been achieved	Peer reviewers	Direct
Reviewing course effectiveness and planning for improvement.	Program Leaders - Faculty	Direct

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

G. Specification Approval Data:

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	