



Jordan University of Science and Technology
Faculty of Computer & Information Technology
Cybersecurity Department

CY381 Risk Management - JNQF Level: 7

Second Semester 2023-2024

Course Catalog

3 Credit Hours. This course discusses how to find and control risks in information assets using risk identification, assessment and analysis, and control approaches. Moreover, it covers malicious human behavioral factors that harm information systems. In this course you will learn about risk management, corporate governance, IT risk assessment, risk monitoring, risk identification, risk analysis, risk evaluation, risk treatment, risk response and reporting, and how to implement and manage a risk management program.

Teaching Method: On Campus

Text Book

Title	Cyber-Risk Management
Author(s)	Atle Refsdal, Bjornar Solhaug, Ketil Stolen
Edition	1st Edition
Short Name	Ref #1
Other Information	

Course References

Short name	Book name	Author(s)	Edition	Other Information
Ref #2	All-in-one CRISC Certified in Risk and Information Systems Control	Peter H. Gregory, Dawn Dunkerley, Bobby E. Rogers	2nd Edition	
Ref #3	Security Risk Management: Building an Information Security Risk Management Program from the Ground Up	Evan Wheeler	1st Edition	

Instructor

Name	Dr. Hala Hamadeh
------	-------------------------

Office Location	CH1 L2
Office Hours	
Email	hmhamadeh@just.edu.jo

Class Schedule & Room
Section 1: Lecture Time: Sun, Tue, Thu : 10:30 - 11:30 Room: A2122

Prerequisites		
Line Number	Course Name	Prerequisite Type
1771010	CY101 Cybersecurity Fundamentals	Prerequisite / Study

Tentative List of Topics Covered		
Weeks	Topic	References
Weeks 1, 2, 3	An overview of GRC (Governance, Risk and Compliance). Introduction to risk and risk management. Applying risk management to information security (Cyber Risk Management).	From Ref #1 , From Ref #2
Weeks 4, 5	Risk assessment approaches, analysis methods, Threat and Vulnerability Identification, Likelihood, and Impact analysis.	From Ref #1
Weeks 6, 7	Risk decision strategies, control selection, mitigation planning, and processing exceptions and acceptance.	From Ref #3
Weeks 8, 9	Risk Monitoring and Reporting, Introduction to various risk reporting techniques, including narrative reports, scorecards, graphs, and real-time information feeds.	From Ref #2
Weeks 10, 11	Information Security Frameworks, and Standards NIST Risk Management Framework (RMF), ISO 27001/27002/27701/31000, and COBIT 2019 (ISACA).	From Ref #2
Weeks 12, 13	Threat and Vulnerability Management: Introduction to Threat Modelling, How to Threat Model, Diagramming your Threat Model, Reduction Analysis. Defining Information Security Metrics, Analysis Techniques, Automating Metrics Calculation and Tools, Risk & Compliance Management.	From Ref #3
Weeks 14, 15	Industry case studies: Analyzing real-world cyber incidents	
Week 16	Final project presentation	

Mapping of Course Outcomes to Program Outcomes and NQF Outcomes	Course Outcome Weight (Out of 100%)	Assessment method

Analyze GRC (Governance, Risk, and Compliance); Illustrating the relationships and interdependencies between governance, risk management, and compliance within an organizational context. [1SO1] [1L7K1]	20%	
Evaluate Risk Assessment Techniques; Apply risk assessment methodologies, conduct analysis, identify threats, and assess their impact. [1SO2] [1L7S1]	30%	
Apply Risk Reporting Skills; Effectively communicate and report risks using appropriate techniques. [1SO3] [1L7S3]	15%	
Verify Compliance with Risk Management Frameworks; Describe and verify the applicability and compliance with risk management frameworks [1SO4] [1L7S2]	15%	
Model Threats and Conduct Reduction Analysis; Demonstrate the ability to model threats, perform reduction analysis, and define information security metrics. [1SO2] [1L7S1]	20%	

Relationship to Program Student Outcomes (Out of 100%)					
SO1	SO2	SO3	SO4	SO5	SO6
20	50	15	15		

Relationship to NQF Outcomes (Out of 100%)			
L7K1	L7S1	L7S2	L7S3
20	50	15	15

Evaluation	
Assessment Tool	Weight
First	25%
Second	25%
Project	10%
Final	40%

Policy	
Attendance	Excellent attendance is expected. In accordance with university regulations, students missing more than 20% of total classes are subject to failure. No excuses will be accepted. If you miss class, it is your responsibility to find out about any announcements or assignments you may have missed. Attendance will be recorded at the beginning or end of each class.
Participation	You are expected to participate in class. Participation includes asking and answering questions, raising issues, and suggesting solutions to the discussed problems.
Exams	All exams will be CLOSE-BOOK. The format for the exams is generally as follows: multiple-choice, and short essay questions.
Makeups	Makeup exam should not be given unless there is a valid excuse. Arrangements to take an exam at a time different than the one scheduled MUST be made prior to the scheduled exam time. In accordance with university regulations, students should bring a valid excuse authenticated through valid channels in JUST.

Workloads	Average work-load student should expect to spend is 6 hours/week.
Code of Conduct	Exams need to be done individually. Projects will be done in groups of 4. Copying of another student's work, even if changes are subsequently made, is inappropriate, and such work will not be accepted. Cheating or copying from neighbor on exam is an illegal and unethical activity and standard JUST policy will be applied. All graded assignments must be your own work.

Date Printed: 2024-03-05