



Prince Sultan University
College of Computer and Info Sciences / Department of Information Systems
2nd Semester 2024-2025
COURSE SYLLABUS

1. **Course number and name:** CYS403: Security Risk Management, Governance and Control
2. **Credits and contact hours:** 3 (3,0,1)
3. **Instructor's or course coordinator's name:** Dr. Abeer Mirdad
 - a. **Scheduled Office Hours** Sunday–Monday–Tuesday: **1:00 PM to 2:00 PM**
 - b. **Office Location:** R310
 - c. **Email:** amirdad@psu.edu.sa
4. **Text book, title, author, and year**
 - a. **Primary Text:** Security Risk Management, Building an Information Security Risk Management Program from the Ground Up, Evan Wheeler
 - b. **Other References:**
 - Cyber Security Management: A Governance, Risk and Compliance Framework 1st Edition by Peter Trim and Yang-Im Lee, 2014.
 - Information Security Policies and Procedures: A Practitioner's Reference, Second Edition 2nd Edition by Thomas R. Peltier
 - Information Security Policies, Procedures and Standards: A Practitioner's Reference, By Douglas J. Landoll
 - c. **Electronic Materials:** None
 - d. **Learning Management System:** Moodle available at <https://lms.psu.edu.sa>
5. **Specific course information**
 - a. **Brief description of the content of the course (catalog description):**

This course focuses on establishing the balance between business needs and cybersecurity safeguards. It will concentrate on the importance of Risk Management framework and the detailed practical Risk management framework. Besides, implementing and assessing the security policies, as a risk mitigation technique, will be discussed deeply based on the business requirements. In addition, auditing, governance, controls, compliance, and standards will be covered with proper case studies and exercises.
 - b. **Prerequisites or corequisites:** CYS401
 - c. **Indicate whether a required, elective, or selected elective (as per Table 5-1) course in the program:** Required
6. **Specific goals for the course**
 - a. **Specific outcomes of instruction. The student will be able to:**

CLO 1: Identify the issues and concerns indicative to protecting information, systems and users.

CLO 2: Apply the principles of cyber security risk management and a framework of components: identification, protection, detection, response and recovery.

CLO 3: Evaluate the types of policy, how policy is created, how to implement and manage policy, measurement practices, and audit of policy

CLO 4: Apply cyber security protection mechanisms to help safeguard and protect information, systems and users.

CLO 5: Articulate cyber security imperatives to key decision makers and stakeholders in an organization.

CLO 6: Recognize the importance of compliance and training in information security risk management.

- b. Explicitly indicate which of the student outcomes listed in Criterion 3 or any other outcomes are addressed by the course.

Course LOs #	Student Outcomes		
	Computer Science	Software Engineering	Information Systems
1	1	1	1
2	2	2	2
3	5	5	5
4	6	2	6
5	3	3	3
6	4	4	4

7. Brief list of topics to be covered

- Cybersecurity - Emerging Technologies CLO 1
- Risky business, Security Risk Management, Governance and Control CLO1
- Threat and Vulnerability Management CLO1
- Cybersecurity Policy Framework CLO3
- The Risk Management Lifecycle CLO2, CLO3
- Risk Profiling CLO4
- Formulating a Risk CLO2, CLO4
- Risk Exposure Factors CLO2, CLO4
- Security Controls and Services CLO4, CLO5
- Risk Evaluation and Mitigation Strategies CLO2
- Risk Assessment Techniques CLO2, CLO4
- Cyber Risk Governance and Standards CLO6
- Building a Risk management Plan from scratch CLO5

8. Weight of Assessments

- Quizzes 10%
- Major Exam 20%
- Assignments 10%
- Attendance 5%
- Project 15%
- Final Examination 40%

The Assessment dates can be seen on Moodle.

9. Additional Information

Plagiarism and Academic Dishonesty:



“Plagiarism can be defined as unintentionally or deliberately using another person’s writing or ideas as though they are one’s own. Plagiarism includes, but is not limited to, copying another individual’s work and taking credit for it, paraphrasing information from a source without proper documentation, and mixing one’s own words with those of another author without attribution. In addition, buying a paper or project, or downloading a paper from the Internet, and submitting them as your own are also plagiarism. The penalty for academic dishonesty will bring course expulsion and failure, or even suspension” (Academic Integrity and Syllabus Acknowledgement Form).

Attendance Policies:

The University attendance policy will be strictly followed.

Students that are regularly absent will be given DN warnings.

Students are expected to attend all class sessions and be in class on-time. Attendance is taken during the first 5 minutes of the class. Missing a class session is a student’s responsibility. Missed classes will not be repeated. It is the student’s responsibility to periodically check course website for course content, projects assignments, updates and notifications.

Exam Policies:

It is not possible to reschedule a major exam. If any student missed an assessment, the makeup will be at the end of the semester and all the materials are included (comprehensive assessment). Makeup exams will only be approved in limited cases as stipulated in the university bylaws. Generally, the final exam includes all material covered during the semester (comprehensive).

Assignment/Project Policies:

Students are expected to actively participate in class discussion, activities and online Forums. Students are expected to complete the class assignment and submit the answers during the concerned tutorial session. Late assignments are not accepted.