1University of Texas at Tyler
Soules College of Business
Department of Computer Science
COSC 4364-5364 Cyber Risk Analysis

Subject to Change

Course Information

COSC 4364-5364 Cyber Risk Analysis Spring 2024
Class Meetings will be in-person MWF 1:25-2:20 PM, COB 207
Please note that all Friday classes are online via Zoom, unless otherwise mentioned.

Instructor Contact

Instructor: Sara Memarian Esfahani
Office location: COB 315.16
Zoom Meeting ID: TBA
Office hours: Mondays and Wednesdays 9:30 to 11:00 or on Zoom by appointment
Email: Use the Inbox in Canvas (MUST include COSC 4364-5341 in the Subject Line)
Normally, I will reply to an email within 24 to 48 hours.
To ensure a quick response over the weekends, please email me no later than Friday mornings.
Occasionally I will be unable to respond within that time frame but will inform the class in advance.

Communication Expectations

The most convenient way to communicate with the instructor is through the Inbox in Canvas. Download the mobile app for your convenience.

Discussion Board Communication
Please post general course or assignment questions to the General Course Questions & Answers Discussion Topic. Students are encouraged to respond to their fellow classmates' questions. I will read all discussion postings and add comments/suggestions/questions as necessary to keep the discussion on topic. Specific topic instructions on discussions are provided in the forums when needed.

Canvas Notifications:
Receive instant notifications about course events, such as submissions, discussion messages, and announcements through canvas. Assignments and all deliverables will be graded and returned no later than one week after the due date.

About the Professor/Instructor

Welcome to COSC 4364-5364 Retail Cyber Security. I am Sara Memarian Esfahani, the instructor for this course. I am excited to have you in this course and look forward to learning more about you and your academic career goals while at UT Tyler. Together we will explore a variety of topics within security issues related to information and organizational assets and we will journey through this course together to do great things.

Course Description

In this course, you will explore the critical aspects of cyber risk analysis, starting with information security assessment basics, project definition, and data gathering methodologies. You will engage with practical examples and case studies to understand risk analysis in depth, learning to identify and mitigate potential cybersecurity threats effectively. This course is designed for IT and Computer Science students and those eager to explore the dynamic field of cyber risk in today's digital world.

Course Structure

This course is a F2F course that lasts 15 weeks (1 semester). See the course schedule table at the end of this file and on Canvas.

Course Pre-requisites and/or Other Restrictions
COSC 4325 or COSC 4360 or equivalent

Course Objectives
Upon successful completion of this course, you are expected to:

- Master Information Security Assessment Basics: Gain a fundamental understanding of information security principles and assessments.
- Learn Effective Project Definition and Planning: Acquire skills in defining and planning cybersecurity projects.
- Explore Data Gathering Approaches: Understand various methods for data collection in cyber risk analysis.
- Conduct Thorough Risk Analysis: Learn to perform in-depth risk analysis using practical examples and case studies.
- Develop Risk Mitigation Strategies: Gain the ability to devise and implement strategies to mitigate cybersecurity risks.

Course Topics

1. Course Overview and Introduction
2. Information Security Risk Assessment Basics
3. Project Definition
4. Security Risk Assessment Preparation
5. Data Gathering
6. Administrative, Technical and Physical Data Gathering
7. Security Risk Analysis and Worked Examples
8. Security Risk Mitigation
9. Security Risk Assessment Project Management and Approaches

Required Materials

The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, Third Edition, by Douglas J. Landoll

COURSE REQUIREMENTS AND GRADING:

Your grade will be determined based on your performance on the activities identified below. No make-up for exams, simulations, or homework will be given. It is highly likely that "extra-credit work" will be assigned to individuals as a replacement for, or in addition to, these components. All points will show up in Canvas. Be sure to review the grading schema below to determine your letter grade.

Individual Assignments: Weekly reading of the assigned chapter for each week. All the students are expected to come to class with questions.

Team Projects: Each student will participate in a systems analysis and Security design project as a team member. The objective of the project is to give students hands-on experience of security analysis and through such in-depth analysis and research, the teams will present their findings and offer mitigation strategies, simulating a somehow actual consultancy role in the cybersecurity landscape.

Team: Each team will consist of up to 5 members. It is the responsibility of individual students to find colleagues to work with as a team. Once a team is formed, each member has obligation to stay and function as a productive team member until the completion of the project. Any disputes, conflicts, and problems within a team must first be resolved among the members.

Each team will elect a team leader who will be responsible for coordinating various project tasks and communicating with the instructor. You may also elect or assign different titles to team members, reflecting different duties and specializations. The performance of a team will always be graded as a single unit. However, individual members will receive an adjusted grade at the end of the semester, which reflects the level of contribution as assessed by peers.

Milestone Reports (100 points):
At the end of each important phases of the project, each team will prepare and submit a report that documents all relevant information as specified in the project case.

Milestone	Title	Due*	Points
1	Organization Selection and Initial Risk Assessment	**Feb 10**	100
2	Comprehensive Risk Analysis and Data Gathering	**March 9**	100
3	Mitigation Strategy Development	**Nov 17**	100
4	Presentation and Final Report	**Apr 15-19**	100

*Due dates are subject to change depending on the class progress

Presentation and Demonstration (50 points):

At the conclusion of the project, each team will make a presentation to demonstrate the system and discuss any relevant issues. The objective of these presentations is to deliver the finished system that meets the needs of the user.
All presentations are in-person, and all the team members are required to participate, regardless of their role in delivery of the presentation.

Final Report (100 points):

Final report collects and organizes all documents prepared and used throughout all phases of the project.
The following is a list of minimum requirements for the report:

- Table of contents
- Executive summary
- Page number on each page (except the cover page)
- All reports and documents collected or produced during the project completion.
- Presentation Slides

Peer Evaluation (10 points)- Extra Credit

All members of the team will receive the same grade for the presentation and the report. At the end of the project (after the report has been submitted), the team members will anonymously evaluate each other on their levels of contribution to the project. The result of this evaluation will determine the points each member will receive for the peer evaluation part of the project grade.
In your evaluation, consider the following (but not limited to):

- Did the member complete assigned tasks in a timely manner?
- Did the member complete the tasks correctly and in a professional manner?
- Did the member attend all meetings?
- Did the member actively participate and make valuable contribution during the meetings?
- Did the member encourage others to do well as a team?

Provide your evaluation in Canvas – Peer Evaluation (Team Project) in the Assignments section.

Report Requirements (All Reports)

- All report assignments are due by the end of the due date unless otherwise instructed. No assignment will be accepted after the due date.
- All reports prepared in Word should include a cover page with the following information:
  - ✓ Team name
  - ✓ Names of team members
  - ✓ Title (e.g., Milestone 3 Mitigation Strategies)

- ✓ Class and section (i.e., COSC 4364)
- All pages except the cover sheet must be numbered.

EXAMS: There will be three exams during the semester. You will be tested on all material assigned or taught in this course which includes class slides, quizzes, videos, etc. Respondus Lockdown Browser & Monitor is required to take all exams which require a webcam feature. Instructions are posted on canvas.

CLASS QUIZZES, ATTENDANCE, AND PARTICIPATION

Regular and punctual attendance for the full class period is expected. Attendance will be recorded. You must attend the entire class to avoid being recorded absent. Any student whose absences exceed the equivalent of two weeks of the class without proper notice may be dropped by the instructor with a WF for nonattendance.
You are expected to come to class prepared. That means you will need to read the assigned chapters and other materials before coming to class and be fully prepared to actively engage in discuss with the class. Friday classes will occur via zoom, and are focused on the review of the week, it can be in a form of pop-up quiz or Q&A.

If you find that there is no grade recorded for submitted work, or if you want to dispute a grade, you must send your instructor an email about the problem NO LATER THAN 2 DAYS after the submission date.

GRADE CRITERIA: All course work is always due at 11:59 p.m., unless otherwise noted. If you have not finished your projects, submit whatever you have completed. You will earn credit for what you complete.

Assignments (Subject to change)	**Points Possible (Approx.)**
Class Quizzes, Attendance, and Participation	150
Team Project	400
Exam 1	150
Exam 2	150
Exam 3	150
Total Points Possible with no extra credit	**1000**

Total Points (%)	**Letter Grade**
900 & above	A
800 - 899	B
700 - 799	C
600 - 699	D
599 & below	F

Schedule (subject to change)
Due by Saturday 11:59 p.m. unless otherwise noted.

Week	Date	Topic / Reading	Note
Week 1	1/17 1/19	Course Overview Introduction	• Understanding the Syllabus • Introduce Yourself
Week 2	1/22 1/24 1/26	Chapter 1&2- Information Security Risk Assessment Basics	• Chapter 1&2 Review on Friday • Project team formation • Decision on your project topic

Week 3	1/29 1/31 1/2	Chapter 3- Project Definition Chapter 4- Security Risk Assessment Preparation	• Chapter 3 and 4 Review on Friday • Milestone 1 due February 10
Week 4	1/29 1/31 2/2	Chapter 5 - Data Gathering Chapter 6 - Administrative Data Gathering	• Chapter 5 and 6 Review on Friday
Week 5	2/12 2/14 2/16	Exam 1- Chapters 1-6	• Exam Review on Monday 12th • Exam day: Wednesday • Exam Evaluation Friday 16th
Week 6	2/19 2/21 2/23	Chapter 7 - Technical Data Gathering	• Chapter 7 Review on Friday • Q&A on Project
Week 7	2/26 2/28 3/1	Chapter 8 - Physical Data Gathering	• Milestone 2 due Saturday March 9th • Chapter 8 Review on Friday
Week 8	3/4 3/6 3/8	Chapter 9 - Security Risk Analysis Chapter 10 - Security Risk Analysis Worked Examples	• Chapter 9 and 10 Review on Friday
Week 9	3/11 3/13 3/15	Spring Break- No Class Meeting	
Week 10	3/18 3/20 3/22	Exam 2- Chapters 7, 8, 9, 10	• Exam Review on Monday 18th • Exam day: Wednesday • Exam Evaluation Friday 22nd
Week 11	3/25 3/27 3/29	Chapter 11 - Security Risk Mitigation	• Chapter 11 Review on Friday
Week 12	4/1 4/3 4/5	Chapter 12 - Security Risk Assessment Reporting	• Chapter 12 Review on Friday
Week 13	4/8 4/10 4/12	Chapter 13 - Security Risk Assessment Project Management	• Chapter 13 Review on Friday • Milestone 3 due on Friday 17th
Week 14	4/15 4/17 4/19	Chapter 14 - Security Risk Assessment Approaches	
Week 15	4/22 4/24 4/26	Team Projects Presentation	• Milestone 4 due • Exam Review on Friday 1st
Week 16	5/1	Final Exam Chapters 11, 12, 13, 14	• No class meeting on Monday April 9th

Code of Conduct and Ethics

Academic integrity must be exhibited in your academic work, methods and conduct. Course work for which you receive an individual grade must be your original, individual effort. If any evidence exists of copying, cheating, or any other forms of academic dishonesty on all, or part, of your graded course work, you (and any others involved) will be awarded a ZERO for that work. Sharing files also counts as academic dishonesty. A second incident will result in a grade of an "F" in this course and a recommendation for further action by the office of the Vice President for Student Development.

A few key points to remember:

I would like to point out some of the activities we have sanctioned (awarded "F" grade and sometimes even more, removed from dean's list, merit list etc.). I want to share this so that you know that we careintegrity of the degree you receive from UT Tyler.

1. In one of the semesters, some exams were conducted using Respondus lockdown browser and video monitoring. However, some students took advantage of a loophole and had help from resources outside the screen and camera. Our instructors viewed 120 hours of video recording and found a group of students involved in a coordinated plagiarism. All were sanctioned, with some losing even scholarships!
2. In one instance, a student outsourced all his assignments to a person outside this country. The assignments were flagged for abnormal activities and with the help of some technology providers we were able to trace the IP address. The student was sanctioned (awarded a "F" grade in the course))
3. In multiple instances, students have had to borrow a laptop from another student in the course and posted something as them because they had not logged out of Canvas. This is considered misconduct on the part of both students. DO NOT give another student access to your UTTyler accounts.

Almost exams and quizzes have multiple versions, and the numbers and options are different. So, if you use your peer – the chance of choosing the wrong answer is extremely high. In worst cases (it has happened in some instances), the student would have used the numbers and details.

The instructor will post both UNOFFICIAL grade reports using Canvas.

THREE BEFORE ME RULE: If you have any issues or questions about assignments, class policies and schedules, etc. and want to speak with me (the Professor), please remember the three before me rule as stated in the next sentence. You must have attempted at least three options before you come to me. For example: TA, tutor, grader, etc. You must tell me what you tried and the results, including screen prints of errors or printed error messages.