CIS 260: SECURITY ASSESSMENT AND RISK MANAGEMENT

Class Schedule:	Tuesday, Thursday 11am to 12:50pm
Instructor:	Chad Johnson
Office:	SCI B231
Email:	Chad.Johnson@uwsp.edu
Office hours:	Tuesday and Thursday, 1pm to 2pm

COURSE DESCRIPTION

Security assessment and risk management is one of the most critical business processes of Information Assurance. Knowing what to protect is required before you can even begin to ask how to protect it. This course will present the topic of security assessments and how risk management works in an organization.

COURSE OBJECTIVES

- Identify vulnerabilities, risks, and threats.
- Appropriately assess and contextualize security risks.
- Formulate and affect risk management strategies.

TEXTBOOK

- *Managing Cyber Risk*, 1st ed, 978-0367177744, by Ariel Evans from Routledge.
- We will be using open-source texts, posted to Canvas.

LECTURES

- Lecture notes will be posted in Canvas. I make every effort to make my notes available, but I may decline to include them at my discretion.
- Students are strongly encouraged to attend each class and actively participate in class discussions.
- In general, I do not believe in taking attendance. However, class attendance may be taken in any class without notification in advance.

GRADING

- 2 Exams: 40% (20% each)
- 6 Labs: 60% (10% each)

Final grades will be assigned according to the following scale:

A: score >= 90	A-: 87 <= score < 90	
B+: 83 <= score < 87	B: 80 <= score < 83	B-: 77 <= score < 80
C+: 73 <= score < 77	C: 70 <= score < 73	C-: 65 <= score < 70
D: 60 <= score < 65		
F: score < 60		

Scale may be adjusted, depending on the overall performance of the class.

ASSIGNMENTS AND DEADLINES

- Labs will be a variety of tasks. Some may require writing a short paper. Others might require completing multiple steps to achieve a goal (as in a CTF.) Each assignment will have those expectations detailed in the assignment instructions.
- Exams/Quizzes are open note/book, and you can use the Internet to search for answers. Please do not collaborate on them. They are not group assignments. You will have the week to complete the exam. Two attempts. Questions will be randomly chosen from a bank. Multiple-choice, multi-select, and true/false only. If you miss an exam, it cannot be made up.

OFFICE HOURS POLICY

- I prefer that you contact me via email.
- Virtual office hours available by appointment

REGRADING

Grades will be posted in Canvas. After the scores are announced, you have 7 days to request regrading by contacting the instructor (office hours or email). Your grade will be final after 7 days.

CANVAS

The Canvas URL is https://canvas.uwsp.edu. Use your UWSP NetID and password to login. We use Canvas for everything from important announcements, instructions, assignment submissions, and grades.

ACADEMIC INTEGRITY

The university cannot and will not tolerate any form of academic dishonesty by its students. This includes, but is not limited to cheating on examinations, plagiarism, or collusion. **Any form of academic dishonesty may lead to F grade for this course.**

STUDENTS WITH DISABILITIES

If you require accommodation based on disability, please let me know. I am willing to provide any reasonable accommodations you require. The sooner you inform me the better.

TENTATIVE SCHEDULE

Week	Lecture Topics	Due	Read
1	Information Risk		
2	Threats and Vulnerabilities	Lab 1	
3	Defense in Depth		
4	Security Strategy	Lab 2	
5	Risk & Impact Assessments		
6	Risk management Frameworks	Lab 3	
7	Security & Risk Tools		
8	Residual Risk	Exam 1	
9	Protection Profiles		
10	Compliance & Regulations	Lab 4	
11	Governance		
12	Validating and Communicating Risk	Lab 5	
13	Business Continuity and Disaster Recovery		
14	Information Criticality	Lab 6	
15	Case Studies		
16	Finals Week	Exam 2	