**ISM 6328**

**Information Security and Risk Management**

Credit Hours 3

USF Muma College of Business

**COURSE SYLLABUS**

Last Updated: 8/4/2023

---

Semester: Fall 2023
Dates: 10/16/23-12/07/23
Delivery Method: Online Course

Instructor: C. Jordan Howell, PhD.
Instructor Email: cjhowell@usf.edu
Office Hours: By appointment

---

## I. Welcome

Hello, and welcome to Information Security and Risk Management! This document contains everything you need to be successful in this course so, if you are reading it, you are on the right path. My name is Dr. C. Jordan Howell, but you can address me as "Jordan" or, if that makes you uncomfortable, "Professor".

The easiest way to get in touch with me is through my USF e-mail. Don't hesitate to reach out if you have any questions, concerns, or simply want to have a casual conversation about cybercrime and cybersecurity. I'm here to assist you and always up for a chat! □

## II. University Course Description

Introduction of frameworks to assess IT risk and implement IT general controls; development of technical skills to secure computer networks.

## III. Required Texts

Textbook (required): Title: Fundamentals of Information Systems Security, Fourth Edition, David Kim; Michael G. Solomon, Paperback: ISBN: 9781284251333, eBook: ISBN: 9781284244571 (includes access to virtual labs).

Supplementary readings and resources: Will be provided on Canvas.

## IV. Course Prerequisites

No prerequisites or co-requisites.

## V. Course Background, Purpose, and Objectives

Cyber-attacks cost the global economy $445 billion annually and affect a variety of domains such as healthcare, government, academia, and industry. Recent years have seen an unfortunate and disruptive growth in the number of cyber-attacks. To stem this grand societal issue, there are increasing calls for well-trained cybersecurity professionals, with an estimated 3.5 million cybersecurity job openings by 2021. Despite this high demand, there is currently a severe shortage of qualified candidates. Specifically, individuals lack technical skills such as planning/implementing/upgrading/monitoring emerging technologies, incident response, security controls, and basic systems administration. Moreover, candidates often lack the non-technical skills of researching and reading new technologies, regulatory compliance, internal security policies, standards, and procedures. This hands-on, introductory, graduate-level course, backwards engineered with DHS/NSA key knowledge unit requirements for maintaining the Center for Academic Excellence for Cyber Defense (CAE-CD) at USF, aims to alleviate these concerns and help students be prepared to become competitive candidates in the field by:

1. Introducing the importance of information security and related business concerns
2. Providing key definitions and terminology for information security
3. Making students aware of the major categories of information security threats
4. Making students aware of the common information security controls
5. Enabling students to implement the basic information security controls
6. Introducing students to the important legal provisions regarding information security
7. Making students aware of the methodological implications for INFOSEC arising from these legal provisions
8. Providing students with an understanding of the standard methodologies for complying with legal requirements for IT general controls
9. Providing basic understanding of IT risk management in organizations
10. Developing valuable skills (e.g., critical thinking) currently in demand for cybersecurity professionals

Upon completion of this course, students will have a strong enough foundation to pursue advanced studies (with additional work, of course!) to attain popular cybersecurity certifications such as Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), Security+, Certified Information Systems Security Professional (CISSP), and SANS GIAC Security Essentials (GSEC). Specifically, students will:

11. 1. Demonstrate an understanding of security concerns and issues in organizations.
12. 2. Learn how to identify and characterize assets relevant to cyber security.
13. 3. Have the ability to identify major categories of information security threats.
14. 4. Have the ability to apply various kinds of controls to counter common threats.
15. 5. Learn about important compliance requirements related to cybersecurity.
16. 6. Have the ability to provide solutions to mitigate IT risks.

## VI. Grading Scale

| Grading Scale (%) | |
|---|---|
| 90-100 | A |
| 80 - 89 | B |
| 70 - 79 | C |
| 60 - 69 | D |
| 0 - 59 | F |

## VII. Grade Categories and Weights (go with Canvas)

| Assessment | Percent of Final Grade |
|---|---|
| Quizzes | 30% |
| Virtual Labs/Assignments | 45% |
| Discussions | 10% |
| Project | 15% |

## VIII. Assignments

**Quizzes:** There are no exams on the course. Such examinations are not necessarily realistic of what you will encounter in day-to-day "real world" working environments (short of professional certifications). Instead, there is a quiz for each chapter. These quizzes are an opportunity to check your knowledge and understanding of each chapter. Security professionals are frequently required to work in a real-time fashion where they may not have the opportunity to look up answers to questions from their boss or co-workers. You will often find yourself in meetings in which time is of utmost importance. The review questions provided at the end of chapter and lecture will help you prepare for the quiz. **Each quiz must be completed individually.**

**Virtual Labs/Assignments:** While the quizzes test your "on the spot" and "quick thinking ability" (both skills highly sought after by security recruiters!), assignments simulate the projects security professionals often engage in. My job is to facilitate your learning – I cannot treat you like an empty glass and just fill you up with knowledge.

As such, the assignments are more critical thinking and hands-on in nature. The emphasis is APPLYING the core knowledge competencies attained in each chapter in meaningful (i.e., recent and relevant) situations. This can and will include the opportunity to apply the course content to areas of your interest and to your workplace environment.

**Discussions:** Since this is an asynchronous online course (we do not have lectures), class participation will be conducted using the Discussion forums in Canvas. The discussion topics can be started by me or by any student. This could be about something you read in the textbook where you want to hear what others think, or maybe a difficulty you faced completing an assignment, or an experience you had that relates to either the chapters or the labs. You can start a new discussion thread with a question, an opinion, an anecdote, a suggestion, etc., or contribute to an existing thread. It is very open-ended, as long as it is something of value to the class. To get full credit for participation (10% of the total grade), I expect you to contribute to a discussion every week. Class participation won't start until week 2 so that you have time to set up the labs and in general get started with the class during week 1.

**Class Project:** A project description will be posted on Canvas during the first half of the course.

## IX. Standard University Policies

Policies about disability access, religious observances, academic grievances, academic integrity and misconduct, academic continuity, food insecurity, and sexual harassment are governed by a central set of policies that apply to all classes at USF. These may be accessed at:
https://www.usf.edu/provost/faculty/core-syllabus-policy-statements.aspx

## X. Course Policies: Attendance

USF requires attendance at the first class so that the university can effectively utilize classroom space and ensure that all students have maximum opportunity to enroll in classes where demand exceeds availability of seats.

YOUR FIRST DAY ATTENDANCE in this class will be measured by the completion of the assignment in the first module titled: “MANDATORY First Day Attendance!! DUE Wednesday by 8:00 a.m.”

**Important: ANYONE not completing this assignment by the due date will be dropped from the course – NO EXCEPTIONS!!!**

## XI. Course Policies: Grades

**Late Work:** Given the accelerated nature of the course, late work will not be accepted.

**Extra Credit:** There will be no extra credit available for the course.

**Grades of Incomplete:** The current university policy concerning incomplete grades will be followed in this course. Incomplete grades are given only in situations where unexpected emergencies prevent a student from completing the course and the remaining work can be completed the next semester. Your instructor is the final authority on whether you qualify for an incomplete. Incomplete work must be finished by the end of the subsequent semester or the “I” will automatically be recorded as an “F” on your transcript.

**Grading Turnaround:** I will make every effort to provide timely feedback on assignments and assessments, aiming to have all submissions graded within one week of the respective due dates. However, please note that unforeseen circumstances or exceptionally high workload may occasionally result in slight delays, and I appreciate your understanding in such cases.

## XII. Course Policies: Technology and Media

**Email**: USF e-mail is the best way to contact me. I will make every attempt to respond to your e-mail within 24-48 hours of receipt. When e-mailing me, be sure to email from your USF student account and please put the course number in the subject line. In the body of your e-mail, clearly state your question. At the end of your e-mail, be sure to put your first and last name, and your university identification number.

**Canvas**: This course will be offered via USF's learning management system (LMS), Canvas. If you need help learning how to perform various tasks related to this course or other courses being offered in Canvas, please view the following videos or consult the Canvas help guides. You may also contact USF's IT department at (813) 974-1222 or help@usf.edu.

## XIII. Course Policies: Syllabus

If necessary, some components of this syllabus may change. However, any such changes will be announced to students in class, on the course website (my.usf.edu – the Canvas site), or via email. The student is responsible for any such announced changes.

## XIV. Schedule

| Week | Required Readings | Assessments** | Lab or Assignment** |
|---|---|---|---|
| 1 | Syllabus<br>Chapter 1: Information Systems Security | Quiz 1 (ch 1) | Exploring the Seven Domains of a Typical IT Infrastructure |
| 2 | Chapter 3: Risks, Threats, and Vulnerabilities<br>Chapter 4: Business Drivers of Information Security | Quiz 3 (ch 3)<br>Quiz 4 (ch 4) | Performing a Vulnerability Assessment |
| 3 | Chapter 5: Networks and Communications Chapter 6: Access Controls | Quiz 5 (ch 5)<br>Quiz 6 (ch 6) | Performing Packet Capture and Traffic Analysis |
| 4 | Chapter 7: Cryptography<br>Chapter 8: Malicious Software and Attack Vectors | Quiz 7 (ch 7)<br>Quiz 8 (ch 8) | Assessing Common Attack Vectors |
| 5 | Chapter 9: Security Operations and Administration<br>Chapter 10: Auditing, Testing, and Monitoring | Quiz 9 (ch 9)<br>Quiz 10 (ch 10) | Implementing an IT Security Policy |
| 6 | Chapter 11: Contingency Planning Chapter 12: Digital Forensics | Quiz 11 (ch 11)<br>Quiz 12 (ch 12) | Performing Incident Response and Forensic Analysis |
| 7 | Chapter 13: Information Security Standards Chapter 14: Information Security Certifications | Quiz 13 (ch 13)<br>Quiz 14 (ch 14) | Red Team On-Site |
| 8 | Chapter 15: Compliance Laws Course wrap-up (Please note that assignments for this week will be due on Friday, not Sunday! This is due when the 8- week course ends). | Quiz 15 (ch 15) | Class Project |