USF Muma College of Business
UNIVERSITY of SOUTH FLORIDA

ISM 6328
Information Security and IT Risk Management
Credit Hours: 3

COURSE SYLLABUS

Semester : Summer 2023
Class meetings : This is an Online asynchronous course.
Instructor : Federico Giovannetti
Contact : fgiovannetti@usf.edu
Office number : N/A, please email me.
Office : N/A
Office Hours : By appointment – in MS Teams
Teaching asst : TBA
TA office hours : By appointment – in MS Teams

University Course Description:

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

Course Prerequisites:

None.

Readings and Resources:

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.

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:

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

Requirements:

Technical: Full-time access to a personal computer (Mac or PC is fine). We also assume that you have a technical background before entering this course (as per the requirements for the MS in Cybersecurity program). This includes basic systems administration, shell scripting, and knowledge about computer networking.

Non-technical (more important!): Capability, aspiration, and positive attitude for learning. Strong work ethic. Interest in information security; it's a hands-on, contact sport!

Course Workload Expectations:

Any university course requires a large amount of work outside of lecture. This course is structured around 8 weeks. Given this condensed time-frame, you should expect a heavier than normal workload. This is a fast-paced course! We assume you will allocate an average of at least 10 – 15 hours per week for study, quizzes, and lab work. **It is your responsibility to manage your workload.** If you procrastinate, you may find that you do not have enough time, or that a technology problem is preventing you from completing your submissions on time. Note that technology problems (such as computer or network failures) will not be accepted as acceptable excuses.

Course Schedule:

Week	Required Readings	Assessments**	Lab or Assignment**
1	Syllabus 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 Chapter 4: Business Drivers of Information Security	Quiz 3 (ch 3) Quiz 4 (ch 4)	Performing a Vulnerability Assessment
3	Chapter 5: Networks and Communications Chapter 6: Access Controls	Quiz 5 (ch 5) Quiz 6 (ch 6)	Performing Packet Capture and Traffic Analysis
4	Chapter 7: Cryptography Chapter 8: Malicious Software and Attack Vectors	Quiz 7 (ch 7) Quiz 8 (ch 8)	Assessing Common Attack Vectors
5	Chapter 9: Security Operations and Administration Chapter 10: Auditing, Testing, and Monitoring	Quiz 9 (ch 9) Quiz 10 (ch 10)	Implementing an IT Security Policy
6	Chapter 11: Contingency Planning Chapter 12: Digital Forensics	Quiz 11 (ch 11) 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) 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

**All deliverables are due at the end of day (11:59 PM) on the submission date (usually Sunday).

Grading:

There are 100 points total in this class. Given the nature of the four core activities which comprise the final grade (detailed below), no extra credit/curves will be provided in this class. Grades will not be rounded up (i.e., 86.9 is a B+, not an A-). The grading breakdown is as follows:

Total points	Grade	Total points	Grade	Total points	Grade	Total%	Grade
>=93	A+	>=83	B+	>=70	C+	>=60	D+
>=90	A	>=80	B	>=67	C	<=57	D
>=87	A-	>=77	B-	>=63	C-	<57	F

Four activities make up the total grade: quizzes, lab assignments, discussion forums participation, and the class project. The point breakdown for each is provided in the table below. The following sub-sections describe each component and summarize the rationale and intuition behind the assessment.

Activity	Type	Individual % Value
Quizzes	Individual	30%
Labs / Assignments	Individual	45%
Discussion Participation	Individual	10%
Project	Individual	15%

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.**

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.

Discussion Forum Participation:

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. The learning objective of the assigned project will be to demonstrate the application of one or several cybersecurity concepts. Sometimes, depending on the type of project, there may be two deliverables (like a midterm and a final). This would help you avoid a heavier load towards the end of the course.

Please note that the quizzes and assignments are not searching through course content and explicit mentioning of every point by an instructor (e.g., control + f). As a master's level course, the assignments require independent thinking (careful thought, critical thinking) and some external research. This simulates what cybersecurity professionals must do on a daily basis – thus, this type of learning cannot be compromised in this class, nor others.

Late Assignment Submission Policy: No late assignments will be accepted. No assignments will be dropped. All assignments must be submitted on Canvas by the due date. **These assignments can take time, please plan your work accordingly.**

Course Hero / Chegg Policy: The USF Policy on Academic Integrity specifies that students may not use websites that enable cheating, such as by uploading or downloading material for this purpose. This does apply specifically to Chegg.com and CourseHero.com – almost any use of these websites (including uploading proprietary materials) constitutes a violation of the academic integrity policy.

turnitin.com: In this course, turnitin.com will be utilized. Turnitin is an automated system which instructors use to quickly and easily compare each student's assignment with billions of web sites, as well as an enormous database of student papers that grows with each submission. After the assignment is processed, as instructor I receive a report from turnitin.com that states if and how another author's work was used in the assignment. For a more detailed look at this process visit http://www.turnitin.com.

Working Ahead of Schedule and Steps to be Successful in this Course:

Each discussion topic, assignment, and quiz will be posted a minimum of one week in advance of their respective due dates. If content opens earlier, students are encouraged to work ahead. If you submit your assignment before the due date, I **might** be able to give you corrective feedback. Students are encouraged to stay in consistent contact with the instructor regarding their progress. To be successful in this course, students are suggested to follow the below strategy (in order) for each week.

1. Carefully read each chapter in the textbook assigned to the week (required reading).
2. Consult with instructor and/or TAs regarding course content if you have any questions.
3. After doing the above two, go over the review questions and take the quiz (independently!).
    a. You are responsible for ALL content in chapter and labs – they will be tested accordingly!!!
4. Carefully work on assignment content following ALL directions carefully and thoroughly.

Office Hours and Communications:

Please email me with any course questions. Selected course questions may be redirected to the course TA(s). **For all emails, please include ISM 6328 in your subject line.** This will enable me to sift through our emails more quickly. Under normal circumstances, I will respond within 24 hours of your post Monday through Friday and 48 hours on Saturday and Sunday. If you have a question regarding your personal performance in the course, please email me directly using the address above. I will provide feedback on course work that needs to be manually graded (e.g., essay papers, projects) within 72 hours of the submission due date. You will be able to see results for automatically graded course work (online quizzes) after the specified deadline.

End of Semester Student Evaluations:

All classes at USF make use of an online system for students to provide feedback to the University regarding the course. These surveys will be made available at the end of the semester, and the University will notify you by email when the response window opens. Your participation is highly encouraged and valued. I take evaluations and feedback extremely seriously. Please also feel free to reach out to me during the semester if you have any feedback – it is better if I know sooner rather than later! Students will have an opportunity to provide feedback at the end of each assignment. The feed-forward assignment is also an opportunity to provide detailed feedback to the instructor.

University Mandated Course Policies:

USF has a set of central policies related to student recording class sessions, academic integrity and grievances, student accessibility services, academic disruption, religious observances, academic continuity, food insecurity, and sexual harassment that **apply to all courses at USF**. Be sure to review these online at: https://www.usf.edu/provost/faculty-success/resources-policies-forms/core-syllabus-policy-statements.aspx

Course FAQ:

How to communicate with me?

You can either send me an email directly or through Canvas. When emailing directly or through Canvas, please write the appropriate subject and include your name at the bottom of the email. The emails should be composed professionally, and the language should be courteous and respectful. I cannot guarantee a response through Teams, specially on weekends.

How NOT to communicate with me?

1. Please do not email me from a non-USF email account.
2. Please do not submit deliverables to me through email. All deliverables must be submitted through Canvas.
3. Please do not reply to an email that I sent to the entire class without changing the subject line, unless your question is about that subject. If you are using the "Reply" button as a means to get my email address in the "To" line, please change the subject line and also delete all previous text from that email, if your email pertains to something else.

How will I communicate with you?

I will send announcements through Canvas. The announcements should arrive in your inbox. If you send me an email through Canvas, I will respond back through Canvas. If you send me an email

directly, I will respond back to your email address. I will make every attempt to reply to your emails within 24 hours during weekdays. I cannot guarantee a response within 24 hours on weekends. Occasionally emails do tend to go to my Junk Mail folder so if you have not received my response within 24 hours, please resend your email directly. I will provide feedback on your assignments through Canvas.

How to Succeed in this Class?

- **Check Canvas and emails daily for announcements:** I will periodically send emails and announcements. I encourage you check them daily.
- **Read the syllabus:** I want to make sure that you understand the course structure and expectations and have your questions answered on the first week. This will help us all have a more productive semester. Please read this syllabus by end of the first week and ask me questions.
- **Complete the reading assignments and class pre-work:** You will get a lot more out of this class if you complete the assigned readings and do the pre-work. In my experience, students who don't complete the reading either never complete it or try to cram it all in just before the exams. That doesn't work. Most of the time, unsatisfactory grades are due to procrastination than any other cause. Please give yourself ample time each week to complete the work for this class.
- **Do not procrastinate on completing assignments:** You cannot pass the course without doing at least most of the assignments. The homework assignments build upon one another. If you get behind, you will find it very difficult to catch up.
- **Do not cheat:** Cheating will not be tolerated. You will lose the entire grade for the assignment and second chances will not be given. Student integrity is a serious matter.
- **A simple formula:** submit quality work, on time.