Course Information

Course Number:	CSCE 477/CSCE 703/ CYBR 403/CYBR 603
Course Title:	Cybersecurity Risk
Section:	CSCE 477/500; CSCE 703/600/CYBR 403/500/CYBR 603/600
Time:	TR 3:55 p.m. – 5: 10 p.m.
Location:	Zach 310
Credit Hours:	3

Instructor Details

Instructor:	Paula S. deWitte, J.D., Ph.D., P.D.
Office:	Peterson 225
E-Mail:	paula.dewitte@tamu.edu (best way to communicate)
Office Hours:	Thursday 2 p.m. – 3 p.m. or by appointment – in person or by zoom

Copy the TA, Stuart Nelson on emails related to assignments, exams, and general course questions
s.s.nelson@tamu.edu

Course Description

Credits 3. (3-0). Risks in cybersecurity; avoidance, acceptance, mitigation, or transference strategies; developing reliable cybersecurity risk assessments to include analysis, categorization, and evaluation; cybersecurity risk audit frameworks.

Course Prerequisites

Prerequisite: Junior or senior classification for undergraduates; or by permission of instructor.

Special Course Designation

N/A

Course Learning Outcomes

At the end of this course, the student should be able to:

- Demonstrate the common body of knowledge for risk assessment in cybersecurity.
- Explain the specialized knowledge for cybersecurity risk applied to current cybersecurity risk issues including supply chain, privacy, and critical infrastructure.
- Develop an understanding of the basic tools and techniques used in risk assessment in cybersecurity of information systems including FEDRAMP templates, NIST Privacy Framework, NIST Cybersecurity Framework, and supply chain.
- Synthesize content into completing risk assessments on sample case studies.
- Explain the significance of cybersecurity risk to enterprise risk.
- Perform risk assessments according to FEDRAMP, NIST Privacy Framework,

Textbook and/or Resource Materials

Textbook: How to Measure Anything in Cybersecurity Risk, Douglas W. Hubbard & Richard Seiersen, ISBN: ISBN-13: 978-1119085294.

Additional reading materials will be posted on the learning management system for this course beginning with:

OPM vs APT: How Proper Implementation of Key Controls Could Have Prevented a Disaster at https://www.sans.org/white-papers/36852/

Essential References:

NIST Controls:

1. NIST SP 800-53 R5, SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST Risk Management Framework:

2. NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management (ERM), https://csrc.nist.gov/publications/detail/nistir/8286/final
3. NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
4. NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and , Organizations: A System Life Cycle Approach for Security and Privacy, https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
5. 3. NIST SP 800-39, SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View,
6.
7. https://csrc.nist.gov/publications/detail/sp/800-39/final
8. NIST SP 800-181 R1, Guide for Developing Security Plans https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final

FEDRAMP (use these templates!)

9. **https://www.fedramp.gov/**
10. **https://www.fedramp.gov/documents-templates/**

CMMC 2.0

11. https://www.acq.osd.mil/cmmc/docs/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

DISA Privacy Impact Assessment (PIA)

12. https://www.disa.mil/~/media/Files/DISA/About/Privacy-Office/DD_Form_2930_PIA_Sections_1-2.pdf

NIST Supply Chain:

13. https://csrc.nist.gov/Topics/Security-and-Privacy/cyber-supply-chain-risk-management

14. NISTIR 8272: Impact Analysis Tool for Interdependent Cyber Supply Chain Risks, https://csrc.nist.gov/News/2020/nistir-8272-published SP 800-53B
15. NIST SP 800-53B, Control Baselines for Information Systems and Organizations, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf
16. NISTIR 8276 (Draft)
17. Key Practices in Cyber Supply Chain Risk Management: Observations from Industry, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8276-draft.pdf
18. NIST SP 800-161 R1 (Draft): Cyber Supply Chain Risk Management Practices for Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft

NIST Privacy Framework: https://www.nist.gov/privacy-framework and https://www.nist.gov/privacy-framework/resource-repository

19. NIST Privacy Framework, https://www.nist.gov/privacy-framework
20. NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf
21. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

NIST Critical Infrastructure Framework:

22. Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/.
23. https://csrc.nist.gov/publications/detail/white-paper/2018/04/16/cybersecurity-framework-v11/final
24. White Paper: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Other Sources:

GDPR:

25. https://gdpr-info.eu/
26. https://gdpr.eu/

Grading Policy

We will utilize the Google Classroom Learning Management System for this course. *

The student's semester grade will be based on assignments, papers, exams, class attendance, and class participation. This course includes extensive in-class hands-on "workshop" type exercises. Class attendance is essential for student success; therefore, students are required to promptly and regularly attend all their classes. A record of attendance will be maintained from the first day of classes and/or the first day the student's name appears on the roster through final examinations and will contribute to the participation grade for the course. Absences may only be excused as defined by the *Texas A&M University Student Rules* available at http://student-rules.tamu.edu/rule07.

This course is stacked with CSCE 703/CYBR 603. Graduate students should enroll in those courses rather than CYBR 403/CSCE 477. **In addition to all undergraduate (CYBR 403/CSCE 477) work, graduate students will have additional requirements for the Semester Paper (i.e., longer paper, more references).**

Requirement:	**Undergraduate Points:**	**Graduate Points:**
10 Assignments (30 pts each) 5 individual; 5 group each assign	300	300
Exam #1	200	150
Semester Paper (Individual)	200	300
Semester Project (Group)	100	100
Exam #2	200	150

Five of the 10 assignments are individual assignments; five of the 10 assignments are group assignments. The rubric for the semester paper/project is included at the end of this document.

Points Grading Scale:
Out of 1000 assignable points
A = 900-1000 points
B = 800-899 points
C = 700-799 points
D = 600-699 points
F = <600 points

Late Work Policy

Late work is work that is not turned in according to the class process by the assigned due date. The instructor may accept late work if the student notifies the instructor BEFORE the assigned due date except In truly emergency situations.

Typically, late and/or make-up work will not be accepted without a university excused absence. If an absence is excused, then the student will be provided an opportunity to make up any homework assignments, quizzes, exams, or other work that contributes to the final grade with a due date that extends the original due date by the number of days of the excused absence. Individual arrangements will be made for exams and quizzes missed due to an excused absence. In all cases, TAMU Student Rule 7 will govern the process.

Course Schedule

Course Topics, Calendar of Activities, Major Assignment Dates
(subject to change as necessary)

Date	Topics	Assignment Milestones
Week 1 Aug 25 Lecture	**Begin: Why Cybersecurity Needs Better Measurements for Risk** Introduction to Course & Expectations; Introduction to Semester In-Class Workshops *What is risk?* Introduction to Risk Management An Overview of Major Incidents that did not properly consider risk.	**Textbook Chapter 1: The textbook is very readable, and we will read through the textbook the first six weeks or so of the semester to establish a basis for our semester work. We may not discuss topics from the textbook, but you need to read it nonetheless.** **Besides the textbook, you need to become familiar with the extensive NIST documentation regarding risk.** **OPM vs APT: How Proper Implementation of Key Controls Could Have Prevented a Disaster at https://www.sans.org/white-papers/36852/**
Week 2 – 1 Aug 30 Lecture	Continue Introduction to Risk Management; Overview of NIST Documentation (NIST SP 800-53 R5 and NIST SP 800-30) available on-line: Be sure to (1) download the most current version – even if in draft form and (2) understand how each document contributes to the NIST approach to risk. **We will begin with SP 800-30 Appendix L and then do an example of the PS Family from NIST SP 800-53 R5.**	**Textbook Chapters 2 and 4 and other readings as assigned.** **Assignment 1 (Individual):** Research a risk in a domain or industry other than cybersecurity and summarize in a one-to-two page paper on that risk. **Due in one week.**
Week 2 – 2 Sept 1	Continue overview of NIST Documentation (NIST SP 800-53 R5 and NIST SP 800-30) available on-line: Be sure to (1) download the most current	**Textbook Chapter 3 and other readings as assigned.**

Lecture	version – even if in draft form and (2) understand how each document contributes to the NIST approach to risk. Prepare for the risk assessment: Overview of setting up a risk project. (template provided) In class example of SP 800-30 and SP 800-53. Introduction to FEDRAMP templates.	**Supplemental posted reading on Enterprise Risk Management** **In-Class Group/Group Discussion (15 – 20 minutes; no group credit).** **Develop a project plan using SP 800-30 Appendix L for in-class problem.** **For in-class discussion/no group credit.**
Week 3-1 Sept 6 Lecture	Continue with FEDRAMP templates.	**Textbook Chapter 5 and other readings as assigned.**
Week 3 – 2 Sept 8 Lecture/In-Class Group	Privacy Walk through complete risk assessment and PIA (Privacy Impact Assessment). There are many PIA templates. We will use the DHS Template found at https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_template.pdf.	
Week 4-1 Sept 13	Review all materials to date. **Be sure you know at this point, how to use the NIST controls (SP 800-53 R5) and FEDRAMP templates to build a risk assessment.** **Walk through NIST SP 800-53 controls in risk assessment in detail.**	**Textbook Chapter 6 and other readings as assigned.** **In-Class Group/Group Discussion (15 – 20 minutes; no group credit):** **Read through ACME company description and list risk categories.** **For in-class discussion/no group credit.**
Week 4-2 **Sept 15**	**Professor on Travel.**	**In-Class Group Assignment 1 (for Credit):** **Each group will be assigned NIST control families. With those families, construct a risk assessment based on the ACME Company.** **Due at 11:59 p.m. September 15, 2022.**
Week 5 – 1	**Begin: Evolving the Model of Cybersecurity Risk**	**Textbook Chapter 7 and other readings as assigned.**

Sept 20 Lecture	Overview of SP 800-39 and SP 800-37: How do these documents fit in with SP 800-30?	**Assignment 2 (Individual):** Write a paper on a specific NIST family of controls (pick out three controls from a control family) assuming medium/moderate data criticality. Develop the NIST risk assessment for those controls (which may take several pages) using a template. The important part of this assignment is to think through any risk issues that should be considered in implementing the controls. For example, what are critical success factors to proper implementation? Due date given in class.
Week 5 – 2 Sept 22 Short Lecture/Workshop	In-class ACME workshop. No lecture. Continue reading.	**Textbook Chapter 8: The book discusses only Bayesian analysis for cybersecurity risk (Chapter 8). This is useful information for the data analytics group assignment.** **In-Class Group Assignment 2 (for Credit):** Derive a PIA for the ACME Company. Due date given in class.
Week 6 – 1 Sept 27 Lecture	Introduction to Supply Chains,	
Week 6 – 2 Sept 29 Workshop	In-class ACME workshop. No lecture. Continue reading. Exam #1 – Material to date – Due date given in class	**In-Class Group Assignment 3 (for credit):** Develop a supply Chain model for ACME. Due date given in class. **Exam #1:** 20% of course grade CSCE 477/CYBR 403 15% CSCE 703/CYBR. Due one week after posting.
Week 7 – 1 Oct 4	Enterprise Risk Management: Integrating Cybersecurity Risk into ERM – Strategic, Financial, and Operational.	**Textbook Chapter 9 and other readings as assigned.** **NISTIR 8286**

	Overview of NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management (ERM). Discussion of class projects.	**Integrating Cybersecurity and Enterprise Risk Management (ERM).**
Week 7 – 2 Oct 6	In-class ACME workshop. No lecture. Continue reading. Select your group and class project topic.	**Textbook Chapter 10 and other readings as assigned.** This begins an ongoing workshop topic.
Week 8 – 1 **Oct 11**	**No class on Tuesday, October 11, 2022.** **Fall break.**	
Week 8 – 2 Oct 13	In-class project workshop. No lecture. Continue reading.	**In-Class Group/Discussion: Present semester project topic to class. 5-minute limit on presentation. Will have slides template for discussion.**
Week 9-1 Oct 18	Overview of SP 800-171 and CMMC. Begin in-class project presentations.	**In-Class Group/Discussion: Present semester project topic to class. 5-minute limit on presentation. Will have slides template for discussion.**
Week 9-2 Oct 20	in-class project presentations. No lecture. Continue reading.	**In-Class Group/Discussion: Present semester project topic to class. 5-minute limit on presentation. Will have slides template for discussion.**
Week 10– 1 Oct 25	Special Topics in Cybersecurity Risk: Critical Infrastructure	
Week 10 – 2 Oct 27	In-class project workshop. No lecture. Continue reading.	**In-Class Group/Assignment 4 (group):** Using a format of your choice (e.g., Excel spreadsheet), develop a template for a cybersecurity risk assessment framework including a sample of risk factors related to cybersecurity

		and enterprise risk (e.g., reputation) related to your group's focus. The template should capture the inter-relationships between the risk factors. As well, define any residual risk and the factors pertaining to those risks. Due date given in class.
Week 11 - 1 Nov 1	Special Topics in Risk: Supply Chain NIST SP 800-161 R1	
Week 11 – 2 Nov 3	In-class project workshop. No lecture. Continue reading.	**Assignment 3 (Individual):** Research an issue related to the risk of protecting critical infrastructure from one of the SSAs and write a one-to-two page paper on summarizing that issue (after class discussion). Start be selecting the critical infrastructure sector of interest. Due date given in class.
Week 12 – 1 Nov 8	Data Analytics in Cybersecurity Risk: Statistical Methods Data Analytics in Cybersecurity Risk: Monte Carlo Simulation; Bow-tie Method Using System Logs and other data in Risk Assessments Other RISK Frameworks: SANS Top 20 Controls and CIS Top Twenty	
Week 12 – 2 Nov 10	In-class project workshop. No lecture. Continue reading. Exam #2 – due in one week	**Exam #2:** 20% of course grade CSCE 477/CYBR 403 15% CSCE 703/CYBR. Due one week after posting. **In-Class Group Assignment 5 (for credit):** Select a risk assessment from our class examples and write a summary on what type of data analytics best matches that particular risk assessment. Include the process for collecting, cleansing, and analyzing the data Due date given in class.

Week 13 - 1 Nov 15	Semester in-class Case Study Discussion & Presentations	
Week 13 – 2 Nov 17	Semester in-class Case Study Discussion & Presentations	**Assignment 4 (Individual):** Select a non-NIST framework and write a one-to-two pager comparing and contrasting that framework with NIST. **Due in one week.**
Week Nov 22	Semester in-class Case Study Discussion & Presentations	
Nov 24	Thanksgiving! Have a great holiday!	
Week 14 -1 Nov 29	Semester in-class Case Study Discussion & Presentations	**Assignment 5 (individual):** Summarize what you have learned about risk in this class and how you will use this going forward. **Due date given in class.**
Week 14-2 Dec 1	Semester in-class Case Study Discussion & Presentations	
Week 15 - 1 Dec 6	Semester in-class Case Study Discussion & Presentations (if necessary) Review of Course; New Topics in Risk in Fall 2022 Course Evaluations; Wrap-Up;	

Attendance Policy

The university views class attendance and participation as an individual student responsibility. Students are expected to attend class and to complete all assignments.

Please refer to Student Rule 7 in its entirety for information about excused absences, including definitions, and related documentation and timelines.

Makeup Work Policy

Students will be excused from attending class on the day of a graded activity or when attendance contributes to a student's grade, for the reasons stated in Student Rule 7, or other reason deemed appropriate by the instructor.

Please refer to Student Rule 7 in its entirety for information about makeup work, including definitions, and related documentation and timelines.

Absences related to Title IX of the Education Amendments of 1972 may necessitate a period of more than 30 days for make-up work, and the timeframe for make-up work should be agreed upon by the student and instructor" (Student Rule 7, Section 7.4.1).

"The instructor is under no obligation to provide an opportunity for the student to make up work missed because of an unexcused absence" (Student Rule 7, Section 7.4.2).

Students who request an excused absence are expected to uphold the Aggie Honor Code and Student Conduct Code. (See Student Rule 24.)

Academic Integrity Statement and Policy

"An Aggie does not lie, cheat or steal, or tolerate those who do."

"Texas A&M University students are responsible for authenticating all work submitted to an instructor. If asked, students must be able to produce proof that the item submitted is indeed the work of that student. Students must keep appropriate records at all times. The inability to authenticate one's work, should the instructor request it, may be sufficient grounds to initiate an academic misconduct case" (Section 20.1.2.3, Student Rule 20).

You can learn more about the Aggie Honor System Office Rules and Procedures, academic integrity, and your rights and responsibilities at aggiehonor.tamu.edu.

***NOTE**: Faculty associated with the main campus in College Station should use this Academic Integrity Statement and Policy. Faculty not on the main campus should use the appropriate language and location at their site.*

Americans with Disabilities Act (ADA) Policy

Texas A&M University is committed to providing equitable access to learning opportunities for all students. If you experience barriers to your education due to a disability or think you may have a disability, please contact Disability Resources in the Student Services Building or at (979) 845-1637 or visit disability.tamu.edu. Disabilities may include, but are not limited to attentional, learning, mental health, sensory, physical, or chronic health conditions. All students are encouraged to discuss their disability related needs with Disability Resources and their instructors as soon as possible.

***NOTE**: Faculty associated with the main campus in College Station should use this Americans with Disabilities Act Policy statement. Faculty not on the main campus should use the appropriate language and location at their site.*

Title IX and Statement on Limits to Confidentiality

Texas A&M University is committed to fostering a learning environment that is safe and productive for all. University policies and federal and state laws prohibit gender-based discrimination and sexual harassment, including sexual assault, sexual exploitation, domestic violence, dating violence, and stalking.

With the exception of some medical and mental health providers, all university employees (including full and part-time faculty, staff, paid graduate assistants, student workers, etc.) are Mandatory Reporters and must report to the Title IX Office if the employee experiences, observes, or becomes aware of an incident that meets the following conditions (see University Rule 08.01.01.M1):

- The incident is reasonably believed to be discrimination or harassment.
- The incident is alleged to have been committed by or against a person who, at the time of the incident, was (1) a student enrolled at the University or (2) an employee of the University.

Mandatory Reporters must file a report regardless of how the information comes to their attention – including but not limited to face-to-face conversations, a written In-Class Group or paper, class discussion, email, text, or social media post. Although Mandatory Reporters must file a report, in most instances, you will be able to control how the report is handled, including whether or not to pursue a formal investigation. The University's goal is to make sure you are aware of the range of options available to you and to ensure access to the resources you need.

Students wishing to discuss concerns in a confidential setting are encouraged to make an appointment with Counseling and Psychological Services (CAPS).

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the University's Title IX webpage.

***NOTE**: Faculty associated with the main campus in College Station should use this Title IX and Statement on Limits of Liability. Faculty not on the main campus should use the appropriate language and location at their site.*

Statement on Mental Health and Wellness

Texas A&M University recognizes that mental health and wellness are critical factors that influence a student's academic success and overall wellbeing. Students are encouraged to engage in proper self-care by utilizing the resources and services available from Counseling & Psychological Services (CAPS). Students who need someone to talk to can call the TAMU Helpline (979-845-2700) from 4:00 p.m. to 8:00 a.m. weekdays and 24 hours on weekends. 24-hour emergency help is also available through the National Suicide Prevention Hotline (800-273-8255) or at suicidepreventionlifeline.org.

Campus Safety Measures

To promote public safety and protect students, faculty, and staff during the coronavirus pandemic, Texas A&M University has adopted policies and practices for the Fall 2022 academic term to limit virus

transmission. Students must observe the following practices while participating in face-to-face courses and course-related activities (office hours, help sessions, transitioning to and between classes, study spaces, academic services, etc.):

- Self-monitoring—Students should follow CDC recommendations for self-monitoring. **Students who have a fever or exhibit symptoms of COVID-19 should participate in class remotely and should not participate in face-to-face instruction.**
- Face Coverings—Face coverings (cloth face covering, surgical mask, etc.) must be properly worn in all non-private spaces including classrooms, teaching laboratories, common spaces such as lobbies and hallways, public study spaces, libraries, academic resource and support offices, and outdoor spaces where 6 feet of physical distancing is difficult to reliably maintain. Description of face coverings and additional guidance are provided in the Face Covering policy and Frequently Asked Questions (FAQ) available on the Provost website.
- Physical Distancing—Physical distancing must be maintained between students, instructors, and others in course and course-related activities.
- Classroom Ingress/Egress—Students must follow marked pathways for entering and exiting classrooms and other teaching spaces. Leave classrooms promptly after course activities have concluded. Do not congregate in hallways and maintain 6-foot physical distancing when waiting to enter classrooms and other instructional spaces.
- To attend a face-to-face class, students must wear a face covering (or a face shield if they have an exemption letter). If a student refuses to wear a face covering, the instructor should ask the student to leave and join the class remotely. If the student does not leave the class, the faculty member should report that student to the Student Conduct office for sanctions. Additionally, the faculty member may choose to teach that day's class remotely for all students.

Personal Illness and Quarantine

Students required to quarantine must participate in courses and course-related activities remotely and **must not attend face-to-face course activities**. Students should notify their instructors of the quarantine requirement. Students under quarantine are expected to participate in courses and complete graded work unless they have symptoms that are too severe to participate in course activities.

Students experiencing personal injury or illness that is too severe for the student to attend class qualify for an excused absence (See Student Rule 7, Section 7.2.2.) To receive an excused absence, students must comply with the documentation and notification guidelines outlined in Student Rule 7.