(C)ITM 835 – Cyber Risk and Threat Management

COURSE OUTLINE FOR 2025-2026

Prerequisite(s):(C)ITM 820

Faculty/Contract Lecturer Information

- **Faculty/Contract Lecturer Name:**
- **Office Location:**
- **Office Hours:**
- **Phone:**
- **Course Website:** my.torontomu.ca (for courses using D2L)
- **Email Address:** youremail@torontomu.ca

Email Policy

Students are expected to monitor and retrieve messages and information sent through D2L and TMU email on a frequent and consistent basis. In accordance with the Policy on TMU Student E-mail Accounts (Policy 157), Toronto Metropolitan University (TMU) requires that any electronic communication by students to TMU faculty or staff be sent from their official university email account. Communications sent from other accounts may be disregarded.

Course Description

This course provides an overview of internal and external cybersecurity risks to organizations and how they can be managed. This includes identifying threat actors and understanding their motivations and intent, as well as outlining their tactics, techniques, and procedures. The course covers risk assessment methodologies, security controls, regulatory compliance, incident response planning, and the role of cybersecurity governance, as well as the frameworks, international standards, and guidelines that regulate these practices. It explains methods of equipping organizations to make informed business risk decisions, depending on their industries and the maturity level of their security programs.

Teaching Methods

If you are registered in an in-person or a virtual classroom, instruction will take place at scheduled hours, following the approach outlined in D2L Brightspace. If you are registered in a Chang School Distance Education course, please follow the schedule, course outline and learning modules as outlined in D2L Brightspace.

Note: All assessments in this course, regardless of its delivery format, will be held in-person on campus. This applies to in-person, virtual, and online courses, including sections/courses delivered through the Chang School.

This course will incorporate the following teaching and learning methods:

- Regular lectures, prescribed weekly readings, group project work, and discussions are the main teaching activities that occur in this course.
- The quizzes are designed to provide the students practice and progressive skill building that they can apply in the group-based project.
- The group project work allows the students to apply the analytical techniques that group interaction and individual and group presentation skills.
- The instructor will establish an active learning environment by engaging the students in an exchange of relevant questions and ideas. Students should expect a frequent and substantive interaction between the instructor and students and among students in every class.

Course Materials

Textbook and Other Learning Materials:

Title: Stepping Through Cybersecurity Risk Management: A Systems Thinking Approach.
Author: Jennifer L. Bayuk
Publisher: John Wiley & Sons, Inc.
ISBN-Print: 9781394213955
ISBN-Online: 9781394213986
Price: Free online access via TMU library. Otherwise, CA$91.99 e-text, CA$113.99 print text.

Supplementary resources:

- MITRE ATT&CK Framework: Threat actor tactics, techniques, and procedures (TTPs) mapping.
- NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments.
- NIST SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations.
- NIST Cybersecurity Framework (CSF) 2.0: Core functions and implementation tiers.
- CIS Critical Security Controls (v8): Actionable best practices for implementing effective safeguards.

Note: All frameworks and standards are publicly available for download from their respective organizations (NIST, CIS, MITRE). Students will reference these materials throughout the Case Briefs, Tabletop AAR, Executive Risk Memo, and Capstone Project assignments. Additional readings will be provided in pdf format through D2L.

Course Learning Outcomes

Academic Upon successful completion of this course, students will be able to:

1. Identify internal and external cybersecurity risks to an organization.
2. Understand the tactics and motivations of threat actors.
3. Understand the core principles and frameworks of cybersecurity risk management in an enterprise context.
4. Conduct risk assessments to identify potential threats and vulnerabilities in business systems.
5. Evaluate and apply security controls and risk mitigation strategies aligned with organizational goals.
6. Develop and implement incident response and business continuity plans.
7. Navigate regulatory requirements and industry standards related to cybersecurity.
8. Demonstrate a thorough knowledge of regulatory frameworks, international standards, and guidelines.
9. Communicate risk management strategies and policies to stakeholders at all levels of the organization.

Integrity

Academic integrity is integral to your learning, the credibility of your degree or certification, and the integrity of the university as a whole. Senate Policy 60: Academic Integrity defines academic misconduct, provides a non-exhaustive list of examples of behaviours that may be considered as academic misconduct, and explains how academic misconduct concerns are evaluated and decided. The entirety of the policy applies in this course. As well, please note that submitting work created in whole or in part by artificial intelligence tools unless expressly permitted by the faculty/contract lecturer, is considered a violation of Policy 60.

Generative AI Course Policy, Plagiarism Detection, and Virtual Proctoring

Generative AI Course Policy

Use of Generative AI (e.g. ChatGPT, Grammarly, Perplexity, DeepL Translator) to develop or assist with any ideas or material submitted for coursework is expressly prohibited in this course. Use of Generative AI in this manner will be considered a breach of Policy 60.

Turnitin or another originality detection software

Turnitin is a plagiarism prevention and detection service to which TMU subscribes. It is a tool to assist faculty/contract lecturers in determining the similarity between students' work and the work of other students who have submitted papers to the site (at any university), internet sources, and a wide range of books, journals and other publications.

While it does not contain all possible sources, it gives faculty/contract lecturers some assurance that students' work is their own. No decisions are made by the service; it generates an "originality report," which faculty/contract lecturers must evaluate to judge if something is plagiarized.

Students agree by taking this course that their written work will be subject to submission for textual similarity review to Turnitin. Instructors can opt to have student's papers included in the Turnitin database or not. Use of the Turnitin service is subject to the terms-of-use agreement posted on the Turnitin website. Students who do not want their work submitted to this plagiarism detection service must, by the end of the second week of class, consult with their faculty/contract lecturer to make alternate arrangements. Students who choose not to have their papers screened for textual similarity review by Turnitin may be required to submit additional work with their research essay. For example:

- an annotated bibliography of each source used in your paper; and/or
- the first few pages of each cited source used in your paper

Even when an faculty/contract lecturer has not indicated that a plagiarism detection service will be used, or when a student has opted out of the plagiarism detection service, if the faculty/contract lecturer has reason to suspect that an individual piece of work has been plagiarized, the faculty/contract lecturer is permitted to submit that work in a non-identifying way to any plagiarism detection service.

Copyright

The course materials provided to you are copyrighted and may not be shared without my express written permission. Do not share these materials (e.g. course outline, lecture slides, assignment instructions) with others and do not post them on the internet during the course, or at any time after. If you do so, Policy 60 will apply.

Academic Integrity Resources

To learn more about Policy 60 and how to avoid academic misconduct, please review and take advantage of these resources:

- Policy 60: Academic Integrity: https://www.torontomu.ca/senate/policies/academic-integrity-policy-60/
- Academic Integrity Office website: https://www.torontomu.ca/academicintegrity/
- "Academic Integrity in Space" game: https://games.de.torontomu.ca/aio/#/
- "Academic Integrity in Cyberspace!" game: https://www.torontomu.ca/aic/#/
- Student Life and Learning Support: https://www.torontomu.ca/student-life-and-learning/learning-support/

Topics and Course Schedule

Week	Topic	Readings
1	**Foundations & Framework Elements** • Explain core cybersecurity risk concepts. • How framework elements connect across business processes.	Chapter 1
2	**Threat Actors, Networks, and Vectors** • Types, motivations, and capabilities of threat actors. • Threat catalogs, vectors, and zero-day threat networks.	Chapter 2
3	**Cybersecurity Events & Attack Scenarios** • Classification and interpretation of cybersecurity events. • Event evidence, uncertainty, and situational awareness.	Chapter 3
4	**Controls - Policy, Standards, Guidelines, and Implementation** • Policies, standards, and procedures as control structures. • Control selection, automation, and maturity development.	Chapter 4
5	**Assessments - Risk, Control Testing & Validation** • Assessments for evidence, validation, and compliance. • Self-assessments, audits, scans, and penetration tests.	Chapter 5
6	**Issues - Identification, Classification & Remediation** • How issues emerge, are classified, and prioritized. • Planning and managing remediation activities.	Chapter 6
7	**Midterm Examination**	Chapter 1 - 6
8	**Metrics - Measures, KRIs & Performance Tracking** • Building meaningful metrics and indicators. • Tracking performance and reporting cyber risk.	Chapter 7
9	**People - Roles, Governance & Three Lines of Defense** • Security roles, responsibilities, and governance layers. • Human risk, accountability, and oversight functions.	Chapter 8
10	**Risk - Categories, Appetite, Tolerance & Probability** • Risk categories, appetite, and tolerance thresholds. • Assessing likelihood, impact, and reporting risk levels.	Chapter 9
11	**Analysis - Decision Support & Capstone Integration** • Using risk data to support executive decision-making. • Integrating framework elements for enterprise reporting.	Chapter 10
12	**Group Project Presentations & Course Reflection** • Group presentations of final risk management plans. • Reflection on learning outcomes and framework integration.	none

Evaluation

The grade for this course is composed of the mark received for each of the following components:

Evaluation Component	Due Date	Percentage of Final Grade	Anticipated Return Date
Case Briefs (x2, 5% each)	Week 04, and 08	10%	Within two weeks
Tabletop After-Action Report	Week 09	5%	Within two weeks
Executive Risk Memo	Week 10	5%	Within two weeks
Group Project	Week 12	20%	Within two weeks
Midterm Examination	TBA	30%	Within two weeks
Final Examination	TBA	30%	TBA
Final Grade		100%	

Note: Students must achieve a course grade of at least 50% to pass this course.

At least 20% of the grade based on individual work will be returned to students prior to the last date to drop a course in good academic standing. For Winter 2026, this is March 27, 2026.

University Policies

You are reminded that you are required to adhere to all relevant university policies found in their online course shell in D2L and/or on the Senate website. Please refer to the Course Outline Appendix for more detail.

Important Resources Available at Toronto Metropolitan University

- The University Libraries provide research workshops and individual consultation appointments. There is a drop-in Research Help desk on the second floor of the library, and students can use the Library's virtual research help service to speak with a librarian, or book an appointment to meet in person or online.
- Student Life and Learning Support offers group-based and individual help with writing, math, study skills, and transition support, as well as resources and checklists to support students as online learners.
- You can submit an Academic Consideration Request when an extenuating circumstance has occurred that has significantly impacted your ability to fulfill an academic requirement. You may always visit the Senate website and select the blue radio button on the top right hand side entitled: Academic Consideration Request (ACR) to submit this request.
  For Extenuating Circumstances, Policy 167: Academic Consideration allows for a

once per semester ACR request without supporting documentation if the absence is less than 3 days in duration and is not for a final exam/final assessment. Absences more than 3 days in duration and those that involve a final exam/final assessment, always require documentation. Students must notify their faculty/contract lecturer once a request for academic consideration is submitted. See Senate Policy 167: Academic Consideration.
Longer absences are not addressed through Policy 167 and should be discussed with your Chair/Director/Program to be advised on next steps.

- If taking a remote course, familiarize yourself with the tools you will need to use for remote learning. The Remote Learning Guide for students includes guides to completing quizzes or exams in D2L Brightspace, with or without Respondus LockDown Browser and Monitor, using D2L Brightspace, joining online meetings or lectures, and collaborating with the Google Suite.
- FAQs Academic Considerations and Appeals
- Information on Copyright for Faculty and students.
- Information on Academic Integrity for Faculty and students.

Accessibility

- At Toronto Metropolitan University, we are committed to ensuring that all courses are accessible to everyone and to removing barriers that may prevent some individuals from enrolling in courses.
- All technologies and tools used in this course are accessible.
- Students who discover an accessibility barrier with any of the course materials or technologies should contact their faculty/contract lecturer.
- As outlined in Policy 159: Academic Accommodation of Students with Disabilities, students are required to proactively consult with AAS, the faculty/contract lecturer, Department or Faculty, as soon as feasible, including prior to enrolling in a course or program, on any concerns they may have about their ability to meet the essential academic requirements of a course/program.

Academic Accommodation Support

Academic Accommodation Support (AAS) is the university's disability services office. AAS works directly with incoming and returning students looking for help with their academic accommodations. AAS works with any student who requires academic accommodation regardless of program or course load.

- Learn more about Academic Accommodation Support.
- Learn how to register with AAS.
- Learn about Policy 159: Academic Accommodation of Students with Disabilities

Academic Accommodations (for students with disabilities) and Academic Consideration (for students faced with extenuating circumstances that can include short-term health

issues) are governed by two different university policies. Learn more about Academic Accommodations versus Academic Consideration and how to access each.

Wellbeing Support

At Toronto Metropolitan University, we recognize that things can come up throughout the term that may interfere with a student's ability to succeed in their coursework. These circumstances are outside of one's control and can have a serious impact on physical and mental well-being. Seeking help can be a challenge, especially in those times of crisis.

If you are experiencing a mental health crisis, please call 911 and go to the nearest hospital emergency room. You can also access these outside resources at anytime:

- Distress Line: 24/7 line for if you are in crisis, feeling suicidal or in need of emotional support (phone: 416–408–4357)
- Good2Talk: 24/7-hour line for postsecondary students (phone: 1-866-925-5454)
- Keep.meSAFE: 24/7 access to confidential support through counsellors via My SSP app or 1-844-451-9700.

If non-crisis support is needed, you can access these campus resources:

- Centre for Student Development and Counselling: 416-979-5195 or email csdc@torontomu.ca
- Consent Comes First – Office of Sexual Violence Support and Education: 416-919-5000 ext 3596 or email osvse@torontomu.ca
- Medical Centre: call (416) 979-5070 to book an appointment.

We encourage all Toronto Metropolitan University community members to access available resources to ensure support is reachable. You can find more resources available through the Toronto Metropolitan University's Wellbeing Central website.