Toronto Metropolitan University

The Chang School of Continuing Education

TED ROGERS SCHOOL Information Technology Management

(C)ITM 825– Enterprise Information Security

COURSE OUTLINE FOR 2025-2026

Prerequisite(s):(C)ITM 820
Antirequisite(s):(C)ITM 805

Faculty/Contract Lecturer Information

- **Faculty/Contract Lecturer Name:**
- **Office Location:**
- **Office Hours:**
- **Phone:** (416) 979 – 5000, ext.
- **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 takes a deep dive into Information Security from an enterprise perspective including the technology, operational procedures, and management practices needed for a successful implementation of cybersecurity. It covers the standards and best practices mandated in information security design, engineering and operations as well as in-depth topics on implementation and integration of cybersecurity in a unified enterprise framework including application, system and network management, governance, threat and incident management, and business continuity.

Course Details

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: Effective Cybersecurity: A Guide to Using Best Practices and Standards (2019)
Author: William Stallings
Publisher: Addison-Wesley Professional
ISBN: 978-0134772806
Price: $75

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. Explain the structure and components of an enterprise information security framework, including asset security, protection strategies, governance, and oversight mechanisms.
2. Demonstrate an understanding of Information Security Governance and its role in aligning security initiatives with organizational objectives.
3. Describe the principles and methodologies of Information Security Risk Assessment, and apply them in evaluating enterprise-level security risks.
4. Analyze the core functions of Cybersecurity, including the management of people, systems, and assets within an organizational context.
5. Demonstrate knowledge of Technical Security Management, including tools, controls, and best practices for securing enterprise IT infrastructure.
6. Explain the purpose and functions of an Information Security Operations Centre (ISOC) and its role in monitoring and responding to security incidents.
7. Evaluate the implications of emerging technologies, such as Quantum Information Technologies, on enterprise information security strategies and practices.

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: www.torontomu.ca/senate/policies/academic-integrity-policy-60/
- Academic Integrity Office website: 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: www.torontomu.ca/student-life-and-learning/learning-support

Topics and Course Schedule

Week	Topic	Readings
1	**Enterprise Information Security Best Practices** • Explain the foundations of Information security CIA Triad and tools providing confidentiality, authenticity, and integrity. • Understanding the Standard of Good Practice for Information Security. Explaining NIST • Cybersecurity Framework and Security, COBIT 5 for Information Security, and Payment Card Industry Data Security Standards.	Chapter 1 Lecture Notes and Weekly Reading (available in D2L after the lecture)
2	**Security Governance & Information Risk Assessment** • Describing security Governance and Security Management. • Explaining Security Governance Principles and Desired Outcomes and Security Governance Components. • Explaining System Assessment Approaches. Describing Asset, Threat, Control, Vulnerability and Consequences Identifications. • Explaining Risk Analysis, Evaluation, Treatment and Risk Assessment Best Practices.	Chapter 2 Chapter 3 Lecture Notes and Weekly Reading (available in D2L after the lecture)
3	**Security Management & People Management** • Describing the Security Management Function, Security Policy, and Acceptable Use Policy. • Explaining Security Management Best Practices. • Understanding Human Resource Security and Security Awareness and Education.	Chapter 4 Chapter 5 Lecture Notes and Weekly Reading (available in D2L after the lecture)
4	**Information Management & Physical Asset Management** • Describing Information Management and Information Classification and Handling. • Understanding Document and Records Management and Sensitive Physical Information handling. • Explaining Hardware Life Cycle Management. Describing Industrial Control Systems and Mobile Device Security.	Chapter 6 Chapter 7 Lecture Notes and Weekly Reading (available in D2L after the lecture)
5	**System Development & Business Application Management** • Describing System Development Life Cycle. • Understanding System Development Management. • Explaining System Development Best Practices. • Describing Application Management Concepts and • Corporate Business Application Security.	Chapter 8 Chapter 9 Lecture Notes and Weekly Reading (available in

	• Explaining End User Developed Application Security and Business Application Management Best Practices.	D2L after the lecture)
6	**Midterm Examination**	
7	**System Access & System Management** • Explaining System Access Concepts, such as User Authentication, Risk Assessment for User Authentication, Access Control, Customer Access. • Describing Server Configuration, Virtual Servers, Network Storage Systems, Service Level Agreements. • Understanding Performance and Capacity Management, Backup and Change Management.	Chapter 10 Chapter 11 Lecture Notes and Weekly Reading (available in D2L after the lecture)
8	**Network and Communications & Supply Chain Management** • Explaining Network Management Concepts, Firewalls, Virtual Private Networks and IP Security. • Understanding Security Considerations for Network Management and Electronic Communications. • Explaining Supply Chain Management Concepts. • Understanding Supply Chain Risk Management, Cloud Computing and Cloud Security.	Chapter 12 Chapter 13 Lecture Notes and Weekly Reading (available in D2L after the lecture)
9	**Technical Security Management** • Understanding Security Architecture principles. • Understanding different security protections and their roles such as malware protection, Identity and Access Management, Intrusion Detection, Information Leakage Protection, Digital Rights Management, Cryptographic Solutions and Cryptographic Key Management.	Chapter 14 Lecture Notes and Weekly Reading (available in D2L after the lecture)
10	**Threat and Incident Management & Local Environment Management** • Understanding Technical Vulnerability Management, Security Event Logging, and Security Event Management. • Describing how Threat Intelligence works. • Understanding the Security Incident Management Framework and the Security Incident Management Process. • Describing the Emergency Fixes, Forensic Investigations, and Physical Security.	Chapter 15 Chapter 16 Lecture Notes and Weekly Reading (available in D2L after the lecture)
11	**Business Continuity Security & Security Monitoring and Improvement** • Understanding the Business Continuity Concepts, elaborate on Business Continuity Program, Business Continuity Readiness, and Business Continuity Operations. • Describe Business Continuity Best Practices. • Describing of Security Audit.	Chapter 17 Chapter 18 Lecture Notes and Weekly Reading (available in

	• Understanding Security Performance and Describing Security Monitoring and Improvement Best Practices	D2L after the lecture)
12	**Project Presentations** • Project Deliverables: slides, written report, presentations.	D2L

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
Online Quiz (best 4 of 5)	Weeks 2, 4, 6, 9, 11	40%	Weeks 3, 5, 7, 10, 12
Project	Week 12	20%	Within a week
Midterm Examination	Week 6	20%	Within a week
Final Examination	TBA	20%	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 Fall 2025, this is Friday November 14, 2025. For Winter 2026, this is Friday 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.