\NEW GRADUATE PROGRAM PROPOSAL

VOLUME I: PROPOSAL BRIEF

This template is to be used when seeking approval for new graduate programs (doctoral and master's) and/or graduate diplomas (types 1, 2, and 3). All new graduate programs and diplomas must receive a recommendation from the Office of the Provost to move through governance processes. Submit the New Graduate Program Proposal (Volumes I and II) to the Assistant Vice-President, Graduate Studies through the Office of Graduate and Postdoctoral Studies (ogps.graduate.curriculum@uoguelph.ca) who, on behalf of the Provost, undertakes initial review to ensure new programming is consistent with the strategic plans and directions for growth of the university. Academic Units are strongly advised to contact the Manager, Graduate Curriculum in the Office of Graduate and Postdoctoral Studies at the outset of proposal development.

In accordance with the University of Guelph's Institutional Quality Assurance Process (IQAP), proposals for new, **for-credit graduate diplomas** follow the **Protocol for Expedited Graduate Approvals**, meaning they require completion of Volumes I and II of the New Graduate Program Proposal, but do not require external review.

Name of Proposed Program:	Master of Cybersecurity Leadership and Cyberpreneurship (MCLC)
Sponsoring Academic Unit and College:	School of Computer Science, College of Engineering and Physical Sciences Executive Programs, Gordon S. Lang School of Business and Economics
Proposed Start Date:	Fall 2023
Proposal Lead(s):	Ali Dehghantanha, Sean Lyons

A. Program Introduction

1. *Provide a brief description of the proposed program including its main goals, and comment on the appropriateness of proposed degree nomenclature.*

Introduction

One need only turn on the TV, open a newspaper, or click on a link from a suspicious email to know that cybercrime is on the rise. The number of computers and internet-enabled devices in homes and businesses is growing. In turn, the volume and sophistication of cyberattacks and data breaches is increasing each year. Thus, there is a growing urgent need for cybersecurity specialists who can assess threats and vulnerabilities, conduct forensic analyses of cyber incidents, coordinate incident response processes, and act as breach coaches. The University of Guelph's School of Computer Science (SoCS), in collaboration with Computing and

Communication Services (CCS), responded to this unmet need by launching the coursework-based Master of Cybersecurity and Threat Intelligence (MCTI) in 2019.
Now, the growing cybersecurity workforce and the increasing popularity of embedded cybersecurity teams within corporate settings is creating a need for businesses to find qualified leaders who can manage these teams.

To develop leadership in the cybersecurity domain, SoCS and the Gordon S. Lang School of Business and Economics ("Lang") are proposing to launch a Master of Cybersecurity Leadership and Cyberpreneurship (MCLC). This professional graduate program will leverage the University's burgeoning reputation in cybersecurity and success of its MCTI program, along with its expertise in leadership and management, to train the next generation of cybersecurity team leaders.

Main Goals

There are several business-focused master's programs in Canada, the US and internationally that include a cybersecurity leadership or management component. However, the proposed program is unique in its equal focus on cybersecurity and management; as well as its in-depth and specialized training in cybersecurity management, governance, and cyberpreneurship. It will provide students with the unique skillset and experience required to build cybersecurity start-ups, lead cybersecurity teams in companies ranging from start-ups to multinationals, or become cybersecurity thought leaders or policy makers in various levels of government or non-government organizations.

Appropriateness of Degree Nomenclature

The degree designations of MA and M.Sc. are typically reserved for research-based programs. In contrast, the purpose of the proposed master's program is to prepare graduates to lead cybersecurity teams within private or public sector organizations. Thus, neither the MA nor the M.Sc. degree designation are appropriate for this professionally-focused, course-based degree program, which is both novel and interdisciplinary.

The proposed program has a unique focus on how to leverage information technology to commercialize and make available their products and services. It will provide graduates with commercialization skills that complement their leadership repertoire, enabling them to lead innovation within their organizations or helm cybersecurity start-ups. Because graduate programming in the field of cybersecurity leadership is relatively novel, it is important for the degree nomenclature to indicate the nature of the program offering explicitly and concisely.

The proposed program name, *Master of Cybersecurity Leadership and Cyberpreneurship* (MCLC), is derived from its dual focus on cybersecurity fundamentals and organizational leadership, as well as its unique focus on cybersecurity entrepreneurship (i.e., "cyberpreneurship"). This name will ensure that prospective students quickly recognize the program's unique combination of learning outcomes. Also, it will enable potential employers to easily identify the relevance of our graduates' expertise while differentiating it from thesis-based programs.

2. *Explain the rationale for developing the proposed program and identify its relationship to the plans of the Department/School and College and the University's Strategic Framework.*

Program Need

There is an existing significant shortage of cybersecurity professionals. According to TECHNATION, one of Canada's leading national technology industry associations, Canadian businesses and industries are struggling to meet their cybersecurity needs[1]. Similarly, a March 2020 survey of cybersecurity executives at major companies (>2,500 employees) in the US and Canada found that 68% of organizations struggle to recruit, hire, and retain cybersecurity talent.[2] Cybersecurity Ventures found that the number of unfilled cybersecurity jobs grew from 1 million positions in 2013 to 3.5 million in 2021.[3] The need for cybersecurity talent is further evidenced by the recent announcement of an $80-million investment by Innovation, Science and Economic Development Canada to support cybersecurity R&D, commercialization and skills and talent development.[4]

The cybersecurity skills gap is similarly apparent at the leadership level. The speed at which cybersecurity investments are being made makes it difficult for forecasters to agree on exact figures. However, IT analysts concur that global spending on cybersecurity will continue to grow at unprecedented rates, creating a wealth of opportunities for budding cybersecurity leaders. Hicham Faik, Global Chief Information Security Officer at Groupe Attijariwafa bank, predicted that the number of Chief Information Security Officer (CISO) job openings will triple over the next five years.[5] Indeed, the executive search firm Phelps Group identified the "Leadership Gap" as one of the key human capital caps within the cybersecurity sector.[6]

Kevin Magee, Chief Security Officer, Microsoft Canada wrote the following on the state of cybersecurity leadership training programs in Canada: "In our urgency to address the technical needs of the industry, little thought and attention has been given to who will lead this future cybersecurity workforce and bridge the gaps between the technical and business worlds of the organization. This has created a new and perhaps even more complex and challenging skills gap — one of leadership. To make progress in these areas we will need skilled cybersecurity leaders who are able to craft and implement sound strategies to hire, integrate and develop new talent. And who can also raise our profession beyond its current technical limitations,

---

[1] "Cybersecurity Skills Framework," TECHNATION, https://technationcanada.ca/en/future-workforce-development/cybersecurity/cybersecurity-skills-framework/

[2] "Fortinet Survey Finds Widespread Impact from Cybersecurity Skills Shortage," Fortinet, https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-fortinet-survey-skills-shortage.pdf

[3] "Cybersecurity Jobs Report: 3.5 Million Openings in 2025," Cybersecurity Ventures, https://cybersecurityventures.com/jobs/

[4] https://www.canada.ca/en/innovation-science-economic-development/news/2021/05/government-of-canada-investing-to-position-canada-as-a-global-leader-in-cyber-security.html

[5] "The Evolving Role of the CISO," Hicham Faik, https://www.linkedin.com/pulse/evolving-role-ciso-hicham-faik/

[6] "Addressing the Cyber Security Talent and Leadership Gap," Phelps Group, https://phelpsgroup.ca/2020/04/13/addressing-the-cyber-security-talent-and-leadership-gap/

focusing simply on mitigating cyberthreats, to address the more strategic challenges of merging cybersecurity into overall business strategy, operations and culture."[7]

According to a recent PwC survey of Canadian CEOs, the greatest factors influencing their cybersecurity strategy were the increasing complexity of threats, the ever-changing cybersecurity and data privacy regulatory landscape, and vulnerability of their partners to cyber threats[8].

Thus, there is a current need for cybersecurity leaders who not only manage teams but also take a holistic look at a business's cybersecurity strategy. The proposed program will train cybersecurity professionals in how to assess a company's current state of cybersecurity risk, preparedness, and adaptability; navigate the evolving regulatory landscape to lead change instead of reacting to it; and be the change champion required to enact a robust cybersecurity strategy that protects the company's critical information and reputation.

What is more, Canada is lagging countries like the U.S. when it comes to reporting security vulnerabilities in public infrastructure, putting Canadians at risk. Without clearly defined reporting mechanisms, it becomes nearly impossible to identify and fix security flaws. This program will provide the training required for graduates to meaningfully contribute to Canadian cybersecurity policy and catch up to cybersecurity resiliency of other G20 nations.

The Unique Skillset Required by Cybersecurity Leaders

Technical expertise in cybersecurity is becoming more widespread, with the proliferation of programs like the MCTI. Accordingly, there is a concomitant need for graduates with working knowledge of cybersecurity fundamentals with developed leadership and management skills who can lead technical teams, be change champions, inform policies and procedures, and liaise with senior leadership and/or government officials.

Ongoing discussions with the MCTI advisory board, which comprises business leaders from top technology companies, have revealed a growing skills gap specifically in the areas of incident response coaching and cyberpreneurship.

In response to industry demands, the proposed program will be targeted towards technical professionals who want to develop enterprise risk assessment, cybersecurity governance, and breach response competencies. It will develop core technical cybersecurity management skills, including:

- Risk assessment and management
- Security management and governance
- Security audit and IT systems control
- Incident response coaching

[7] "Developing the Security Leaders we Need," Canadian Security, https://www.canadiansecuritymag.com/developing-the-security-leaders-we-need/

[8] https://www.pwc.com/ca/en/ceo-survey/23rd-ceo-survey/the-state-of-cybersecurity-and-privacy.html

At the same time, the proposed program aims to address the more strategic challenges of merging cybersecurity into overall business strategy, operations and culture. It will develop leadership and management competencies relevant to the cybersecurity sector, including:

- Financial Literacy
- Project Management
- Organizational Change Leadership
- Cyberpreneurship

Alignment with the University's Strategic Documents

Consistent with the University of Guelph's 2020-25 Strategic Mandate Agreement with the Province, this program will address a gap in post-secondary offerings and prepare students for successful and fulfilling careers in a rapidly changing world. Specifically, the proposed program will meet the government's calls to action to strengthen the University's economic prospects in the critical area of cybersecurity through interdisciplinary approaches that have come to define innovative programming at Guelph. Upon completion of the proposed program, graduates will be positioned to secure critical job openings and achieve success in the workplace.

The proposed program also responds to several themes in the University of Guelph's Strategic Framework: *Our Path Forward* (2016):

***Stewarding Valued Resources*:** This proposal meets the Framework's call to sustain and cultivate people and facilities to meet the needs of the future. This program will be supported by growing complement of cybersecurity faculty members in SoCS, including three recent hires with expertise in cybersecurity and threat intelligence. These faculty members have brought new energy and research potential to the School. Moreover, this new partnership with Lang will usher new opportunities for interdisciplinary collaborations in areas such as security management, cyberpreneurship, and data analytics.

The Security Operations Centre in CCS was constructed for the purpose of enabling experiential learning activities that familiarize cybersecurity students with industry expectations. The Centre will be used to host remote practice sessions for students in the proposed program, as part of CIS*6710 Principles and Practice of Information Security.

Catalyzing Discovery and Change & Inspiring Learning and Inquiry: The proposed program will promote innovation, adaptation, responsiveness, and resilience in the face of rising in cyber-crimes. It will offer a unique learning environment, with students from diverse backgrounds learning from interdisciplinary team of instructors. Through course discussions, students will tackle complex questions and issues typical of those faced by cybersecurity and management professionals. Moreover, the opportunity to undertake projects with their employers will support the University's goals for widespread adoption of experiential learning activities.

Connecting Communities: This proposed program follows in the University's tradition of cultivating and upholding meaningful, mutually beneficial partnerships within our local and global communities. This program will enhance existing relationships with existing partners

such as Advisory Board members: Arctic Wolf, BlackBerry, BMO, Bruce Power, Canadian Cyber Threat Exchange, Canadian Tire Corporation, Cisco Systems, Crowdstrike Inc., EQ Bank, eSentire, Georgian Partners, IBM, ISA, Long View Systems, Mandiant Canada, McAfee, Microsoft Canada, Orion, Province of Manitoba, RBC, RCMP, Stratejm, The Canadian Centre for Cyber Security, The Co-Operators, Toronto Police, KPMG, DarkTrace, and PWC. These partners will help inform the curriculum to ensure that graduates are well-equipped to meet present and future industry demands for cybersecurity leaders.

Alignment with the College's Strategic Plan: Inspiring Excellence.

To achieve its mission, the 2018-2023 College of Engineering and Physical Sciences (CEPS) Strategic Plan *Inspiring Excellence*[9] outlines six guiding principles to focus its efforts, including leading in learning. A key objective outlined in this theme is to create new professionally oriented master's programs. The proposed program is aimed at targeting an audience of aspiring leaders and working professionals with interest or expertise in cybersecurity. It will equip graduates with the skills and expertise required to become entrepreneurs in the cybersecurity space. It will also strengthen the College's reputation as a national leader in cybersecurity. One of the newest graduate programs developed in CEPS includes the professionally oriented MCTI program[10]. The proposed MCLC program will complement MCTI by providing working professionals who do not necessarily have the technical background required to succeed in MCTI with an opportunity to gain an overview of current challenges and emerging opportunities in cybersecurity, as well as the general leadership skills required to fill growing job opportunities as cybersecurity team leaders and managers.

Moreover, the proposed program's focus on privacy, security, ethics and professional practice also aligns with the College's recent investment in the Centre for Advancing Responsible and Ethical Artificial Intelligence (CARE-AI). It also aligns with recently launched technical graduate programs that focus on ethical application of AI or data science in a variety of application areas (which may include cybersecurity) such as the Collaborative Specialization in Artificial Intelligence and the Master of Data Science.

Alignment with the Lang School of Business and Economics Strategic Plan
Lang's vision[11] is 'to be recognized locally and globally for our commitment to developing future leaders for a more sustainable world.' Reflecting our University's commitment to 'Improve Life,' this vision represents a foundational belief that business can and should be a 'force for good' in the world. This translates into our mission, wherein we seek to view *business as a force for good*® through:

- Pushing the frontiers of knowledge through research in business, management and economics, building on industry foundations unique to the University of Guelph.

[9] https://sway.office.com/eJ9KioD9nmThO1Ld?ref=Link&loc=play

[10] https://www.uoguelph.ca/computing/graduates-graduate-programs/master-cybersecurity-and-threat-intelligence-mcti

[11] https://www.uoguelph.ca/lang/mission-vision

- Fostering the long-term success of our students' career aspirations, organizations and the betterment of society through research-inspired and socially relevant educational programs, which develop teamwork, critical-thinking and problem-solving skills.
- Encouraging an ethos of community engagement and ethical and responsible leadership in a complex and ever-changing world.

The proposed program supports Lang's mission by offering a collaborative vehicle through which leadership capacity can be developed and deployed toward the goal of increasing cybersecurity. Cybersecurity is a fundamental societal issue for the 21st century. Developing leaders with the capacity to tackle this issue is critical to the well-being of businesses and the economy in general, and to the mission of business as a force for good.

Alignment with the School of Computer Science Strategic Direction

The proposed master's program will benefit SoCS in countless ways. A growing cohort of graduate students and closer relations with industrial partners will raise the School's visibility, both within and outside the University community. It will build their alumni network. It will provide opportunities for faculty and MCLC students to secure Mitacs grants in support of students' work internships that simultaneously solve company-specific problems and advance faculty members' research programs. In turn, these industry-faculty collaborations may evolve into larger investments by industry into the faculty's research programs e.g., in the form of matching towards NSERC Alliance grants. The outcomes that result from these research projects will provide content in the form of student success stories and research advancements that can be highlighted in marketing materials that promote the School's programming and research intensity. Marketing this success will help build the School's internal standing, national and international reputation, and catalyze new partnerships that could result in strategic investment in SoCS and its faculty members' research programs. Lastly, any residual revenues that are not reinvested into the MCLC program can be used to resource other aspects of the School's operations that support its faculty's research, teaching and/or service efforts. The proposed program will be a welcomed and powerful addition to the School's current complement of graduate programming.

3. *Describe how relevant stakeholders were consulted in preparing this proposal. If the proposed program includes resources (e.g., courses, faculty supervision) from units other than the sponsoring unit, clear commitments of support for the proposed program must be included in* ***Volume II****.*

The impetus for the proposed program's development was strongly encouraged by industry experts on the MCTI Advisory Board. The MCTI Advisory Board is highly representative of the cybersecurity community, as it includes CISOs and other C-level executives from more than 25 companies and government organizations who prioritize cybersecurity, including Arctic Wolf, BlackBerry, BMO, Bruce Power, Canadian Cyber Threat Exchange, Canadian Tire Corporation, Cisco Systems, Crowdstrike Inc., EQ Bank, eSentire, Georgian Partners, IBM, ISA, Long View Systems, Mandiant Canada, McAfee, Microsoft Canada, Orion, Province of Manitoba, RBC, RCMP, Stratejm, The Canadian Centre for Cyber Security, The Co-Operators, Toronto Police, KPMG, DarkTrace, and PWC. The idea to develop a leadership program in

cybersecurity was first highlighted in the MCTI Advisory Board meeting in August 2019 and it received overwhelming support. Specifically, the Advisory Board's industry and government leaders expressed an urgent need for greater leadership competencies in cybersecurity. Quotes and letters of support from members of the Advisory Board are included in Section H and Volume II.

The need for a cybersecurity leadership program was discussed again in the MCTI Advisory Board meeting of January 2020, in which board members indicated strong support for a new master's program with dual focus on cybersecurity skills and leadership development. They further noted that development of the proposed program should be of high priority so that U of G can gain a competitive advantage by being the first mover in this untapped market.

As a collaborative program, this proposal was developed jointly between CEPS and Lang, with input from members of both colleges. In CEPS, consultation was undertaken within SoCS, whose faculty are the key providers of the cybersecurity content of the program. The cybersecurity faculty members in SoCS were consulted at key checkpoints during proposal development. In May 2022, the SoCS faculty council was briefed on the program's progress. [ND1]

Within Lang, the proposed program was reviewed under the School's policy on new program proposals. Consultation was undertaken with faculty and leadership of the Department of Management, who are expected to be the primary providers of the leadership and entrepreneurship content of the program. The program learning outcomes were also assessed within Lang's AACSB accreditation framework, which incorporates an assurance of learning process.

B. Learning Outcomes and Assessment

1. Outline and describe the anticipated learning outcomes of the proposed program.

The MCLC program is focused on training working professionals to become ethically-minded leaders in cybersecurity and future CISOs in organizations ranging from startups to established multinational companies. The MCLC students will have rich experiential learning opportunities throughout the program's curriculum. For example, in CIS*6710, students work in teams to develop a solution to a real-world security and privacy issue. Some students may seek Program Director approval to pursue an independent integrative learning opportunity where they will be expected to propose, plan, implement, and present an evidence-based solution to a complex company-specific cybersecurity problem in partnership with an industry mentor and faculty supervisor. Moreover, this program will integrate ethical considerations of cybersecurity in each of the below-listed domains to deliver graduates with unique skills and dispositions that will fill the pressing societal need for cybersecurity leaders.

The program-level learning outcomes have been designed in consultation with the MCTI Advisory Board to ensure that all graduates are equipped to assess an organization's IT and business systems, identify and manage enterprise IT risk, manage enterprise IT governance systems, perform cybersecurity audits, and lead incident response coaching. In addition, all graduates will have mastered key business concepts, including financial literacy, project

management, organizational change leadership, and cyberpreneurship. The program-level learning outcomes are as follows:

Security Management and Governance: The practice and design of security governance, program development and management, incident management and risk management along with abilities to assess, design, implement and manage IT governance and business systems. Graduates will be able to:

- Design and implement enterprise security governance programs
- Design, implement and assess enterprise incident and risk management programs
- Assess, design, implement and manage IT governance systems in alignment with business requirements

Security Audit and Information Systems Control: The ability to audit, control, monitor and assess an organization's IT and business systems, identify associated risks, and implement controls to manage those risks. Graduates will be able to:

- Identify and manage enterprise IT risk
- Implement and maintain risk registers and risk controls
- Implement privacy by design to IT systems, networks and applications
- Develop controls: defense controls, offensive controls, investigative controls (digital forensics)

Project Management and Governance: The ability to plan, resource, schedule and control project processes and deliverables, make use of financial information and manage teams to deliver cybersecurity solutions on time and on budget. Graduates will be able to:

- Apply Project Management tools in planning, executing, controlling, and closing a project through its lifecycle.
- Input and analyze key financial information and its implications in consultation with financial managers to affect strategy, operations, and performance.
- Create project management documents related to project scope, plan, schedule, risk, communication, quality, and project closing.
- Optimize a project while managing the triple constraints of time, cost, and scope.
- Report project progress effectively to project stakeholders in oral and written format.
- Use negotiation skills in initiating and managing changes to project scope.
- Identify and analyse the ethical considerations implicit in managing projects, including the potential effects on project owner, sponsor, and users.

Cyberpreneurship and Organizational Change Leadership: The ability to lead organizational change and manage innovation and entrepreneurship within organizations and teams. Graduates will be able to:

- Assess technological solutions with respect to their technical, market and financial feasibility.
- Develop business models and manage projects under high uncertainty.
- Understand and utilize key skills related to entrepreneurship, relationship building, organizational change, as well as project and personnel management.
- Develop a strategy to lead a change effort within an organization;

- Design a process for promoting change in an organization;
- Implement skills related to change management (e.g., communication);
- Identify potential weak points that could undermine a change effort, and address sources of resistance to change;
- Critically analyze new information regarding change that you may encounter; and
- Understand the process and the analytical tools that can assist in the innovation and commercialization process and how best to prepare technologies to survive commercialization.

Professional Capacity: Professional Capacity entails the ability to abide by ethical guidelines, laws, and regulations. It involves the ability of the graduate to work collaboratively and independently in regional and global contexts. Graduates will be able to:

- Demonstrate ethical behaviour consistent with academic integrity and the professional code of ethics as required in cybersecurity and threat intelligence
- Collaborate on and conduct in-depth research about different cyber threats and prepare relevant technical and non-technical reports
- Exercise entrustable professional skills including initiative, responsibility, accountability, and decision making in complex situations

2. *Describe any proposed fields[12], and outline any unique learning outcomes associated with each field. Note: Programs are not required to declare fields at either the master's or doctoral level.*

No fields are proposed as part of this program.

3. *Identify which of the five University of Guelph Learning Outcomes for Graduate Programs are particularly addressed and how the proposed program supports student achievement of the University learning outcomes. Include the Learning Outcome Alignment Template (see "LO Alignment Template" under "Graduate LOS" on the Learning Outcomes website), or a comparable curriculum overview map and learning outcomes table in **Volume II**.*

The proposed program addresses each of the University of Guelph's Learning Outcomes for graduate programs, as outlined in Table 1, below.

TABLE 1. Program, University of Guelph, and OCAV Learning Outcomes

Critical and Creative Thinking	Critical and creative thinking is a concept that refers to the application of logical principles, after much inquiry and analysis, to solve problems with a high degree of innovation, divergent thinking and risk taking. Those mastering this outcome show evidence of integrating knowledge and applying this knowledge across disciplinary

[12] *In graduate programs, "fields" refer to approved areas of specialization or concentration related to the demonstrable and collective strengths of the program's faculty. Roughly one third of a student's program of study should be reflective of their declared field. As such, programs that wish to establish fields are encouraged to include modest course requirements that support the learning outcomes associated with that field, and student research in thesis-based programs should relate to their declared field.*

	boundaries. Depth and breadth of understanding of disciplines is essential to this outcome. At the graduate level, originality in the application of knowledge (master's) and undertaking of research (doctoral) is expected.		
	OCAV GUDLEs	**University of Guelph Learning Outcomes and Associated Skills**	**MCLC Program Outcome Areas**
	1. Depth and Breadth of Knowledge 2. Research and Scholarship 3. Level of Application of Knowledge 4. Professional Capacity / Autonomy 6. Awareness of Limits of Knowledge	Independent Inquiry and Analysis	Security Management and Governance; Security Audit and Information Systems Control; Project Management and Governance; and Professional Capacity
	1. Depth and Breadth of Knowledge 2. Research and Scholarship 3. Level of Application of Knowledge 4. Professional Capacity / Autonomy	Problem Solving	Security Management and Governance; Security Audit and Information Systems Control; Project Management and Governance; and Cyberpreneurship and Organizational Change Leadership
	2. Research and Scholarship 3. Level of Application of Knowledge	Creativity	Security Management and Governance; Security Audit and Information Systems Control; and Cyberpreneurship and Organizational Change Leadership
	1. Depth and Breadth of Knowledge 6. Awareness of Limits of Knowledge	Depth and Breadth of Understanding	Security Management and Governance; Security Audit and Information Systems Control; Project Management and Governance; Cyberpreneurship and Organizational Change Leadership; and Professional Capacity

Literacy	Literacy is the ability to extract material from a variety of resources, assess the quality and validity of the material, and use it to discover new knowledge. This definition also includes the ability to use quantitative data, effective use of technology and the development of visual literacy.		
	OCAV GUDLEs	**University of Guelph Learning Outcomes and Associated Skills**	**MCLC Program Outcome Areas**
	2. Research and Scholarship 5. Level of Communication Skills	Information Literacy	Security Management and Governance; Security Audit and Information Systems Control; Project Management and Governance; and Cyberpreneurship and Organizational Change Leadership
	2. Research and Scholarship 5. Level of Communication Skills	Quantitative Literacy	Security Management and Governance; Security Audit and Information Systems Control; and Project Management and Governance
	2. Research and Scholarship 5. Level of Communication Skills	Technological Literacy	Security Management and Governance; Security Audit and Information Systems Control; and Project Management and Governance
	2. Research and Scholarship 5. Level of Communication Skills	Visual Literacy	Security Management and Governance; and Security Audit and Information Systems Control

Global Understanding	Global understanding encompasses the knowledge of cultural similarities and differences, the context (historical, geographical, political and environmental) from which these arise, and how they are manifest in modern society. Global understanding is exercised as civic engagement, intercultural competence and the ability to understand an academic discipline outside of the domestic context.

	OCAV GUDLEs	University of Guelph Learning Outcomes and Associated Skills	MCLC Program Outcome Areas
	1. Depth and Breadth of Knowledge	Global Understanding	Security Management and Governance; and Cyberpreneurship and Organizational Change Leadership
	1. Depth and Breadth of Knowledge 2. Research and Scholarship 6. Awareness of Limits of Knowledge	Sense of Historical Development	Security Audit and Information Systems Control; and Professional Capacity
	4. Professional Capacity / Autonomy	Civic Knowledge and Engagement	Security Management and Governance; Security Audit and Information Systems Control; and Professional Capacity
	4. Professional Capacity / Autonomy 5. Level of Communication Skills	Intercultural Knowledge and Competence	Security Management and Governance; Security Audit and Information Systems Control; Cyberpreneurship and Organizational Change Leadership; and Professional Capacity

Communicating	Communicating is the ability to interact effectively with a variety of individuals and groups and convey information successfully in a variety of formats including oral and written communication. Communicating also comprises attentiveness and listening, as well as reading comprehension. It is the ability to communicate and synthesize information, arguments, and analyses accurately and reliably.		
	OCAV GUDLEs	**University of Guelph Learning Outcomes and Associated Skills**	**MCLC Program Outcome Areas**
	2. Research and Scholarship 5. Level of Communication Skills	Oral Communication	Security Management and Governance; Security Audit and Information Systems Control; and Professional Capacity

	2. Research and Scholarship 5. Level of Communication Skills	Written Communication	Security Management and Governance; and Security Audit and Information Systems Control
	2. Research and Scholarship 3. Level of Application of Knowledge 5. Level of Communication Skills	Reading Comprehension	Security Management and Governance; and Security Audit and Information Systems Control
	2. Research and Scholarship 3. Level of Application of Knowledge 5. Level of Communication Skills	Integrative Communication	Security Management and Governance; Security Audit and Information Systems Control; and Professional Capacity

Professional and Ethical Behaviour	Professional and ethical behaviour requires the ability to accomplish the tasks at hand with proficient skills in teamwork and leadership, while remembering ethical reasoning behind all decisions. Organizational and time management skills are essential in bringing together all aspects of managing self and others. Academic integrity is central to mastery in this outcome. At the graduate level, intellectual independence is needed for professional and academic development and engagement.		
	OCAV GUDLEs	**University of Guelph Learning Outcomes and Associated Skills**	**MCLC Program Outcome Areas**
	4. Professional Capacity / Autonomy	Teamwork	Security Management and Governance; Security Audit and Information Systems Control; Project Management and Governance; and Professional Capacity
	4. Professional Capacity / Autonomy	Ethical Reasoning	Security Audit and Information Systems Control; Project Management and Governance; and Professional Capacity
	4. Professional Capacity / Autonomy	Leadership	Security Management and Governance;

			Cyberpreneurship and Organizational Change Leadership; and Professional Capacity
	4. Professional Capacity / Autonomy	Personal Organization / Time Management	Project Management and Governance; Cyberpreneurship and Organizational Change Leadership; and Professional Capacity
	4. Professional Capacity / Autonomy	Intellectual Independence	Security Management and Governance; Security Audit and Information Systems Control; Project Management and Governance; Cyberpreneurship and Organizational Change Leadership; and Professional Capacity

4. *Indicate how the identified outcomes will be assessed, and comment on the appropriateness of the proposed methods of assessment in evaluating student progress and achievement of the program learning outcomes.*

The proposed program's curriculum has been designed to enable students to meet all the identified program learning outcomes at a level appropriate for a professionally oriented master's degree. Scaffold assessments and experiential learning opportunities will ensure that students should have demonstrated a high level of achievement by the end of each course. they should build professional and independent capacity in each of the subject areas as they progress through the program.

Evaluation in nearly every course will be a mix of collaborative group and individual work that could manifest in the following ways:

- **Written assignments** that will assess students' practical and theoretical skills, their abilities to research and report risks associated with IT and business assets, and thus their abilities in critical and creative thinking, literacy, communication, and global understanding. For example, in CIS*6720, students will produce a professionally written, high-quality report

that reflects their assessment, design and implementation of an enterprise IT governance program that aligns with an organization's goals and requirements.

- **Case studies** that will assess students' abilities to apply critical and creative thinking, literacy, communication, global understanding, and professional and ethical behavior to resolve problems that are representative of real-world challenges. These will involve investigations of different risks, analyses of a variety of incident management and risk management concepts, and the development of programs and procedures to monitor risks relevant to IT and business assets. For example, in CIS*6710, students work in pairs to research security and privacy issues within real-world systems and apply their knowledge to develop solutions. In CIS*6720, students will learn about security, privacy, legal and ethical risks and develop an information security program that identifies, manages and protects the organization's assets aligned with the organization information security governance framework.

- **Oral presentations** that will assess students' abilities in critical and creative thinking, communication, and professional and ethical behavior. For example, in CIS*6710, students will work in groups to present a real-world case study on how available security technologies to monitor risks and threats to an organization, as well as how to balance an organization's risk appetite versus the recommended people, process and technology controls.

In addition to coursework, some students may complete a 1.0-credit culminating project that will advance knowledge or practice, and address an emerging challenge in security management, cyber governance, cyberpreneurship or a closely related field. Most projects will be completed in conjunction with an industry partner or in collaboration with students in the MCTI program.

Table 2 provides a visual depiction of how the course assessments and outcomes align with the program learning outcomes. Every course in the program will meet at least two of the core program learning outcomes. Within each course, key concepts will be introduced through mini-lectures and case studies, then practiced and reinforced through assessments. Each course concludes with a substantial project or exam that requires integrating course concepts/methods, investigating and analysing findings, designing solutions, and communicating/proposing results. Table 2 also indicates through light green shading that students *may* meet the program learning outcomes by completing a final independent project (CIS*6730 Cybersecurity Management and Governance Project) in lieu of MGMT*6400 Project Management.

TABLE 2. Courses and Program Learning Outcomes

Program Learning Outcome Areas	Courses							
	School of Computer Science				LANG School of Business			
	CIS*6590	CIS*6710	CIS*6720	CIS*6730 (in place of MGMT*6400)	BUS*6180	BUS*6190	LEAD*6200	MGMT*6400

Security Management and Governance								
Security Audit and Information Systems Control								
Project Management and Governance								
Cyberpreneurship and Organizational Change Leadership								
Professional Capacity								

5. Identify any distinctive curriculum aspects, program innovations, or creative components.

This program will feature experiential learning opportunities in which students will analyse real-world scenarios informed by industry partners and/or undertake case studies in collaboration with industry partners. For example, In CIS*6710, students work in teams to develop an innovative solution to a real-world security and privacy issue. In CIS*6720, students complete a practical exam where they are tasked with developing and monitoring an information security program, as well as establishing an incident handling and response procedure strategy based on given assets and potential security loopholes. Moreover, in CIS*6590, students will interact with guest speakers/panels comprised of government and industry cybersecurity experts, and engage in discussions on various emerging issues in cybersecurity, privacy, digital forensics, incident handling, etc. These learning opportunities will provide students with the practical experience desired by prospective employers.

The focus on cyberpreneurship, which is most evident in the course BUS*6190 Cyberpreneurship is a novel feature of this program that positions it at the leading edge of the field. The synthesis of cybersecurity and entrepreneurship represents a defining element of this program – the dual focus on technical and managerial competencies.

Students will also have access to the ever-growing set of professional and career-development opportunities, similar to the ones that are typically provided to students in Lang's executive programs. At present, this includes networking events, professional development workshops, skills assessments and the annual Lang leadership conference. The Lang Executive Programs team is currently developing new and expanded professional and career development programming in conjunction with the Lang Business Career Development Centre and the John F. Wood Centre for Business and Student Enterprise. MCLC students will also have access to programming provided by Lang's centres and institutes, including the Institute for Sustainable Commerce, the International Institute for Sport Business and Leadership, and the Marketing Analytics Centre.

6. *Describe how the curriculum addresses the current state of the discipline. For professional programs, identify congruence with current accreditation and regulatory requirements of the profession and include any formal correspondence with accrediting bodies in* ***Volume II****.*

As noted in the introduction, cybersecurity is a burgeoning professional field with an expected lack of qualified job seekers, not only to fill technical roles but also to fill leadership roles within private sector and government. The proliferation of cybersecurity programs is slowly addressing the need for cybersecurity analysts. But the growing number of cybersecurity analysts embedded within companies is concomitancy expanding the need for skilled cybersecurity professionals who can lead technical teams and interface with company executives; or work with government and non-government organizations to ensure that cybersecurity and privacy governance policies and regulations keep pace with advancements in a rapidly changing field. The proposed program imparts students with the skills required to fill cybersecurity leadership roles. It also features two unique learning outcomes that are in high-demand according to the MCTI Advisory Board: incident response coaching and cyberpreneurship.

The proposed program will be unique in Canada and one of only a handful of programs around the world that prepares students to lead cybersecurity teams in organizations ranging from startups to established multinational companies, and work with or act as cybersecurity regulators. Graduates of the proposed program will be well-equipped to step into information security audit, governance, and management roles in both the private (e.g., financial, manufacturing, and professional services firms) and public (e.g., government, military, health care, etc.) sectors. The following are examples of tasks graduates will be able to perform upon degree completion:

- Audit and compliance reviews and security control assessment
- Incident analysis and reporting
- Identifying and managing enterprise IT risk and implementing system controls
- Security governance program development and management
- Assessment and alienation of cybersecurity programs with business needs and requirements
- Implementing privacy by design and by default into IT systems, networks, and applications
- Enabling digital access to enterprise products and services by leveraging IT
- Apply basic project management and change management tools and techniques such as communications, stakeholder analysis, risk analysis, cost estimation and budgeting, and quality control in an organizational context.

Cybercrime, which is predicted to cost the world $10.5 trillion annually by 2025, up from $6 trillion in 2021, will continue generating new cybersecurity jobs.[13] The 2021 CISO 500, an annual compilation of Fortune 500 CISOs, indicates that every Fortune 500 company now has a CISO role or its equivalent—up from 65% of companies in 2017.[14] A survey from the IDC

[13] “Cybercrime to Cost the World $10.5 Trillion Annually by 2025,” Cybersecurity Ventures, https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[14] “List of Fortune 500 Chief Information Security Officers,” Cybersecurity Ventures, https://cybersecurityventures.com/ciso-500/

sponsored by CapGemini of over 1,000 large enterprise executives across the globe found that 90% of executives surveyed said the CISO is involved in significant business innovation and change decisions.[15] Most CISOs attend board and executive management meetings. Yet, according to a KPMG and Harvey Nash report, only 21% of CISOs believe they're very well-positioned to deal with security risks.[16] The key to being able to respond quickly and proactively to the automated attacks is through intelligence-driven cybersecurity. Today's CISO not only needs to proactively think about the organization's IT security strategy, but also its long-term business strategy. The proposed program uniquely combines instruction and experiences in privacy and threat intelligence with leadership and management fundamentals. It will train the next generation of cybersecurity leaders who can fill important and ever-evolving cybersecurity leadership roles in private sector and government.

C. Program Requirements

The below table represents an example course schedule with sequence of courses and depicting in-person versus remote offerings. As shown in Table 4, students are enrolled in online courses throughout their first two semesters and are required to come to campus for a 10-day intensive course at the beginning of semester 3 (CIS*6720), after which they may take one more course (MGMT*6400 – DE) or complete the MRP course (CIS*6730). Students therefore have the flexibility to complete the program online or to undertake a major research project at their industry mentor's organization (can be their current employer) for their entire third semester. All students are required to take the 10-day intensive course in Semester 3.

TABLE 3. Example course schedule (dates subject to change)

Semester	Start Date	End Date	Offered	Class Schedule	Course Title	Course Code
F23	05-Sept-23	21-Oct-23	Remote	Synchronous	Principles and Practices of Information Security	CIS*6710
F23	22-Oct-23	10-Dec-23	DE (via OpenEd)	Asynchronous	Leadership of Organizational Change	LEAD*6200
F23/W24	05-Sept-23	14-April-24	Remote	Synchronous	Professional Seminar in Cybersecurity	CIS*6590
W24	08-Jan-24	19-Feb-24	DE (via OpenEd)	Asynchronous	Financial & Managerial Accounting	BUS*6180

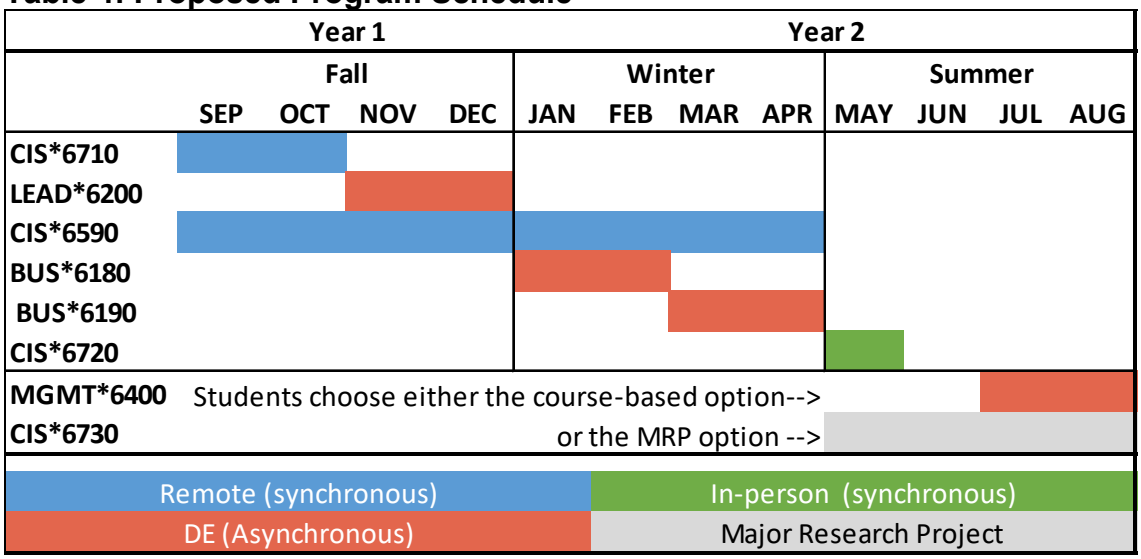
[15] "The Modern, Connected CISO," IDC, https://www.capgemini.com/ca-en/wp-content/uploads/sites/10/2019/01/The-Modern-Connected-CISO-8.pdf

[16] "Navigating Uncertainty," Harvey Nash/KPMG CIO Survey 2017, https://assets.kpmg/content/dam/kpmg/cz/pdf/HarveyNashKPMGCIOSurvey2017_web_access.pdf

W24	25-Feb-24	14-April-24	DE (via OpenEd)	Asynchronous	Cyberpreneurship	BUS*6190
S24	15-May-24	25-May-24	In-person	Synchronous	Cyber Security & Privacy Management and Governance	CIS*6720
S24	17-Jul-24	1-Sep-24	DE (via OpenEd)	Asynchronous	Project Management**	MGMT*6400

**Can be replaced by CIS*6730, which would be completed in May to August, with prework followed by a 12-week internship.

Table 4: Proposed Program Schedule



1. Outline the requirements[17] of the proposed program:

The program requires successful completion of 3.5 graduate credits consisting of: three courses from SoCS (3 x 0.5 = 1.5 credits) and 4 courses from Lang (4 x 0.5 = 2.0 credits). Students who seek approval from the Program Director may opt to take 4.0 graduate credits consisting of six required courses (3 x 0.5 credits from SoCS; and 3 x 0.5 credits from Lang) and a major research project (CIS*6730, 1.0 credit). If students are approved to complete the major research project, then it will be in lieu of MGMT*6400.

Four courses from the School of Computer Science:

- CIS*6590 – **Professional Seminar in Cybersecurity, 0.5 credit**
- CIS*6710 – **Principles and Practice of Information Security (new), 0.5 credit**

[17] *For each required course, provide its calendar description here and include a course outline in **Volume II**. For each new course or revised course proposed as part of this submission, also include a course addition or course change form in **Volume II**.*

- CIS*6720 – **Cyber Security & Privacy Management and Governance (new), 0.5 credit**

Four courses from Lang (0.5 credits each):

- BUS*6180 – **Financial and Managerial Accounting, 0.5 credit**
- BUS*6190 – **Cyberpreneurship (new), 0.5 credit**
- LEAD*6200 – **Leadership of Organizational Change, 0.5 credit**
- MGMT*6400 – **Project Management, 0.5 credit**

Major Research Project course (1.0 credit):
In their third semester, students may register in CIS*6730 Cybersecurity Management and Governance Project in place of MGMT*6400 Project Management, pending Program Director approval. This project course requires a major individual piece of work that demonstrates understanding of and an ability to reason about a specific facet of information security management. Students who are previously employed in the security industry may pursue a project with their former employer or another industry partner.

a. *courses currently offered, with frequency of offering;*

BUS*6180 – **Financial and Managerial Accounting** (annually)
CIS*6590 – **Professional Seminar in Cybersecurity** (annually)
LEAD*6200 – **Leadership of Organizational Change** (annually)
MGMT*6400 – **Project Management** (annually)

b. *new courses proposed as part of the submission;*

BUS*6190 Cyberpreneurship
This course merges the disciplines of entrepreneurship and cybersecurity with a focus on the process of generating and launching new cybersecurity sensitive or dependent ventures. Students who successfully complete this course will be able to assess cybersecurity market opportunities, develop a startup plan, assess risks and ethical considerations and effectively communicate ideas to ensure success of new ventures.

CIS*6710 Principles and Practice of Information Security
This course teaches the foundations of cybersecurity and its applications in cyber risk assessment, identification of cyberattacks and threats, and controls for defenses and recovery. Fundamentals of cybersecurity are covered in sufficient breadth and depth so that the students can analyze systems for weaknesses, design a security policy, and identify controls that will help enforce security policies. Where applicable, real life case studies will be discussed to learn why security systems fail.

CIS*6720 Cyber Security & Privacy Management and Governance
This course offers an overview of privacy legislation and ethical theories/principles and their applications. The course also examines strategies standards, and best practices for privacy and ethical risk assessment, mitigation. compliance, and governance. Moreover, the course introduces state of the art security architecture, incident detection, containment and eradication

and strategies to integrate different security technologies to achieve organization objectives. In addition, it provides a comprehensive review of information security governance framework and supporting processes to manage information risk to an acceptable level. It then looks at methods to build and maintain an information security program that identifies, manages and protects the organization's assets.

c. *required courses mounted by other units;*

N/A

d. *for doctoral programs, the structure of the qualifying examination;*

N/A

e. *required research and/or experiential learning activities; and*

Required Experiential Learning Activities: Experiential learning is a staple throughout the proposed program. For example, in CIS*6710, students work in teams to develop an innovative solution to a real-world security and privacy issue. In CIS*6720, students assess security, privacy, legal and ethical risks using best practices and standardized frameworks and apply regulatory frameworks and standards for data protection and privacy to mitigate risks and enhance compliance. In addition, students develop an information security program that identifies, manages and protects the organization's assets (informed by industry partners) aligned with the organization's information security governance framework. Our industry partners will support experiential learning activities by providing access to highly qualified resources and subject matter experts, informing real-world case studies and/or hosting internships (see letters of support from industry and community partners in Volume II). Notably, all the companies represented on the MCTI Advisory Board have expressed a willingness to support this program, e.g., by providing case studies or hosting student internships.

Optional Experiential Learning Activities: The major research project (CIS*6730) requires that students address a company-specific emerging issue in cybersecurity management, leadership, or a related field. The student will begin their project in the final semester of the program. The project course requires that students pose their own question, approach and secure an industry mentor and faculty supervisor for the project, formulate a plan of action, manage the project timeline, and follow-through with the project such that they produce a rigorous report that demonstrates a sophisticated understanding of challenges in cybersecurity management and governance (or a closely related field) and the ability to integrate ethics, regulations, and best practices, in the development and implementation of a solution. Students will be encouraged by the Program Director to seek their guidance in securing an industry mentor and faculty supervisor.

f. *required thesis, major paper, or other capstone requirement.*

There is not any required thesis or major paper in the proposed program.

2. *Describe the modes of delivery (in-class, lecture, problem- or case-based learning, distance education, hybrid). Explain why the modes of delivery are appropriate for meeting the program's learning outcomes.*

The program will launch with a sequence of five 7-week online courses. Students will also attend a seminar series that runs part-time throughout Fall and Winter semesters, as well as an intensive 10-day on-campus residential course that coincides with the timing of Lang's annual business leaders conference. Beginning in 2022, Lang will host an on-campus conference that will provide students, which provides professional and executive programs students (e.g., Lang's MBA, MA Leadership, Master of Project Management and GDip in Accounting) with the opportunity to engage in various workshops and seminars, as well as interact with guest speakers and their executive program peers. Note that some Students will pursue a major research project in the last semester in lieu of MGMT*6400 Project Management.

The primarily online learning format is critical to meet the target audience's needs for flexibility—it will enable them to meaningfully engage in the course content while pursuing full-time work outside of the program. Asynchronous course components will ensure that all students are able to complete the requirements according to their availability, while meeting regular deadlines to ensure that they are understanding key concepts and methods and keeping pace with their peers. The synchronous on-campus course in Semester 3 and student conference ensures that students have an opportunity to engage with each other, program faculty and the University of Guelph campus during their program.

The optional MRP will take the form of an individual project based on a real-world cybersecurity leadership issue (typically provided by the student's employer) or an internship with an industry partner mentor. In all cases, the student must secure a faculty supervisor and Program Director approval.

Both Schools are committed to meeting the needs of all students and will partner with Student Accessibility Services to develop accommodations when appropriate.

3. *If the program is to allow for part-time study, describe how the delivery differs from that of the full-time program and summarize the pathway to completion.*

To accommodate working professionals, the program will offer a two-year part-time pathway. The mode of delivery does not change for part-time students. There is no designated pathway to completion as none of the courses have prerequisites—they can be taken in any order, enabling maximum flexibility for professional students. However, the Program Director may decline a student's request to take the major research project if they have not demonstrated competencies in the course(s) completed prior to their request. Part-time students may take one or two courses in each semester and should complete the program within 24 months.

4. *Comment on the appropriateness of the program requirements and structure in meeting the program learning outcomes.*

The program structure and curriculum have been thoughtfully designed to provide working professionals with flexibility (part-time or full-time study pathways) and choice of curriculum components (course-only or MRP options), whilst still ensuring that they are able to meet all the identified program learning outcomes in a timely manner. Full-time students will progress through the program by completing two courses in the first semester (Fall); two courses in the second semester (Winter); a seminar series that runs through first and second semesters; and two courses in the third semester (Summer).

It is expected that many students will complete the program by taking the course-only path. However, students may seek the Program Director's approval to complete a major research project (MRP) in lieu of MGMT*6400 Project Management in Semester 3. To be approved for the MRP, a suitable industry project (i.e., with cybersecurity management and governance, and project management components) must have been identified, the student must be selected as the company's top choice following an interview screening process, and a suitable faculty supervisor must agree to act as the project advisor. All students who are pursuing an MRP will be expected to apply for research internship funding via Mitacs Accelerate or similar funding program, which will consist of defining the research problem, and formulating a project management plan.

All students will complete the program with the same learning outcomes. Namely, it is expected that each student who pursues the MRP will complete a real-world cybersecurity management and governance project while exercising project management principles and techniques. Each project will have an industry mentor and an MCLC faculty advisor. Students in the course-only option will gain fundamental project management principles and techniques via MGMT*6400.

The MRP will be advertised as non-compulsory and pending Program Director approval, for several practical reasons: 1) we cannot guarantee that there will be a suitable industry project for every MCLC student; 2) the availability of suitable faculty supervisors will become a bottleneck, depending on cohort size, which can only be addressed by recruiting additional cybersecurity faculty members in SoCS and/or Lang; and 3) many MCLC students will prefer to take the course-only option.

Part-time students will take one or two courses per semester until they complete the program requirements. They are expected to complete the program within 24 months. The courses complement each other, but none are prerequisites for each other. The stand-alone nature of MCLC courses maximizes program flexibility, which is especially important in catering to the needs and interests of working professionals. The absence of lock-step prerequisites should allow for a smoother progression through the program for part-time students. In this way, the intensive, 12-24-month, curriculum will prepare students to fill the growing societal need for cybersecurity leadership in a timely manner.

5. *Describe how student progress will be monitored to ensure timely achievement of milestones (completion of coursework, QEs, etc.).*

As this is a coursework-based program, all courses will include evaluations of student progress consisting of individual and group assignments, projects, and presentations. Final numerical grades will be assigned in all courses (except for CIS*6730). In this way, the Program Director will have semesterly indicators of student progress and the ability to intervene if learning difficulties or systemic issues are identified.

The appropriateness of the assessment methods used within each course has been demonstrated through alignment with the program learning outcomes (see **Table 2**).

D. Admission Requirements

1. *List the admission requirements of the proposed program and indicate their appropriateness for ensuring adequate achievement and preparation for entry into the program.*

To be considered for admission, applicants must:

1. Be qualified graduates of a four-year honour's undergraduate degree or equivalent from a recognized university (minimum B- average); and
2. Have at least two years of relevant work experience as determined by the admissions committee. Applicants should clearly demonstrate the relevance of their work experience in the statement of intent and resume submitted with their application.

Additionally, all applicants must meet the University of Guelph's English Language Proficiency requirements for admission. If an applicant's first language is not English, or their undergraduate degree was not taught at an English-language institution, an English Language Proficiency test will be required. Applications from qualified members of under-represented groups are encouraged.

These requirements are consistent with the University of Guelph's regulations for admission to master's programs.

2. *List any proposed alternative requirements (beyond the University-wide Alternate Admissions Criteria) and rationale.*

N/A

E. Anticipated Enrolment and Impact on Existing Programs

1. *Describe enrolment projections for the proposed program, including:*
    a. *initial enrolment;*

Initial enrolment in Fall 2023 is expected to be 25.

    b. *annual enrolment increases above initial enrolment; and*

Annual enrolment increases are expected to be approximately 5-10 students per year.

c. steady-state—total enrolment, and the year this will be achieved.

It is expected that the program will reach its steady-state enrolment of 40 students by Year 3.

2. *Describe any overlap with existing programs. Discuss potential impacts of the new program on existing programs, whether students may transfer to this program from others, and/or whether the proposed program is expected to attract new students.*

There is no significant overlap with existing programs. The existing courses being used from Lang include one course from MA Lead, one course from MBA, one from the Master of Project Management program and a new course offered through the Department of Management. The existing professional programs available in Lang attract students interested in pursuing general management or leadership education. They are not designed for industry professionals looking to pivot into a cybersecurity career or a cybersecurity expert wanting to further specialize in cybersecurity leadership.

Course content from the MCTI program is being leveraged in this program, but it has been reorganized along with new material to specifically cater to the distinct MCLC student audience and MCLC program learning outcomes. The existing MCTI program is focused on attracting recent computer science and technical graduates whereas the MCLC program is focused on attracting professionals in the workforce.

This coursework-based program is expected to attract new students to the University who are not interested in traditional thesis-based M.Sc. degrees. Instead, prospective students for this program are interested in entering cybersecurity but do not have the necessary technical background for MCTI program, or they are cybersecurity professionals aspiring to secure leadership positions in the field and need the industry-specific knowledge that is unique to the MCLC program (as opposed to MA Lead or MBA).

3. *Are any programs or fields of existing programs proposed for closure because of this proposed new program?*

No programs are proposed for closure because of this new program.

F. Administration

1. *Identify the Graduate Program Coordinator to be responsible for program management and academic counselling.*

Day-to-day operations and routine oversight of the proposed program will be shared by SoCS and Lang.

For the first three years, the current MCTI Program Director, Dr. Ali Dehghantanha, will act as the MCLC Program Director and Graduate Program Coordinator. Dr. Dehghantanha has two-

course teaching relief, providing him with sufficient time to take on this additional administrative assignment. When the program reaches steady-state enrolment, a dedicated Program Director will be appointed for a renewable five-year term. The MCLC Program Director will be responsible for program management and academic counselling. They will be in regular contact with their counterparts in SoCS and Lang to coordinate efforts whenever appropriate.

Program Committee: The MCLC Program Committee will include Dr. Dehghantanha (Chair); two cybersecurity faculty members from Drs. Dara, Khan, Lin and Obimbo; Lang faculty members Drs. Rezania and Burga; a staff member (to be identified); and an MCLC student rep (to be identified). The Program Committee will meet regularly to review student performance, discuss curriculum changes to better align course outcomes with program learning outcomes, or determine ways to improve the overall student experience. They will review and approve any curriculum changes recommended by the Cybersecurity Advisory Board (see below).

Advisory Board: To start, the MCTI Advisory Board will be leveraged to provide advice for the MCLC program and renamed the Cybersecurity Advisory Board to reflect its broader scope more accurately. Most board members have already provided significant input into the proposed program's development and are committed to providing advisory support to the new program. As the MCLC program evolves and program needs diverge, it is expected that the Cybersecurity Advisory Board membership will be split across MCTI and MCLC, with a stronger focus on technical expertise within the MCTI Advisory Board and greater management/leadership focus on the MCLC Advisory Board. The Cybersecurity Advisory Board will keep the MCTI and MCLC Program Directors informed about emerging industry trends, suggest program improvements and modifications, and provide guest lectures and company-specific practice problems.

The MCLC Program Director will receive one-course teaching relief. Moreover, the proposed program will be supported by a dedicated graduate program assistant (GPA), in coordination with existing GPA resources in both SoCS and Lang (roles and responsibilities will be coordinated to mitigate duplication of effort and ensure a consistent client experience); a dedicated Industry Liaison Officer, and 0.5 IT support (shared with the MCTI program). Both colleges will be engaged in marketing, recruitment and admissions. To start, GPA support will come from existing resources in SoCS and Lang. The need for dedicated GPA resources will be evaluated in Year 2. Similarly, an Industry Liaison Officer is already in place for MCTI and will cover MCLC needs in Year 1. The need for additional industry liaison resources will be evaluated in Year 2. In Year 1, IT services will be provided by the CCS team. But, as the program expands, it is envisioned that SoCS or the College of Engineering and Physical Sciences will make available dedicated human resources to support this program's IT needs.

2. *Describe how the program plans to document and demonstrate the level of performance of students in the program as a whole and how this information will be used towards the continuous improvement of the program moving forward.*

Upon acceptance into the program, students will be offered information about available supports. Moreover, the Program Director will check in with course instructors at the end of each term to ensure that students' course performance is aligned with their expectations. The

Program Director will offer to meet with individual students who are not meeting performance expectations to ensure that they are aware of available supports and to offer further guidance, as appropriate.

Any issues that arise more than once will be considered as potential systemic barriers to performance. These issues will be brought to the Program Committee to identify barriers, as well as discuss and implement curriculum changes to mitigate these barriers for future cohorts.

G. Resources

1. *In **Table 5** below, list the core faculty who will provide instruction and supervise within the proposed program. The intent of this Table is to establish the strength and the degree of involvement of the faculty complement participating in the program (whose CVs are provided in **Volume II**). Note: Completed and Current supervisory records need not be recorded if the proposed program does not involve graduate supervision (e.g., coursework master's).*

TABLE 5. Faculty Members

Faculty Name & Rank	Home Unit[1]	Supervisory Privileges[2]	Areas of Expertise[3]			
			1	2	3	4
***Category 1 – Tenured or tenure-track core faculty** members whose graduate involvement is exclusively in the graduate program under review. For this purpose, the master's and doctoral programs of the same name are considered a single program. Membership in the graduate program, not the home unit, is the defining issue.*						
***Category 2 – Non-tenure-track core faculty** members whose graduate involvement is exclusively in the graduate program under review.*						
***Category 3 – Tenured or tenure-track** core faculty members who are involved in teaching and/or supervision in other graduate program(s) in addition to being a core member of the graduate program under review.*						
Rozita Dara - Associate	SoCS	Full	X	X		
Ali Dehghantanha - Associate	SoCS	Full	X			
Andrew Hamilton Wright - Associate	SoCS	Full		X		
Charlie Obimbo - Associate	SoCS	Full	X	X		
Xiaodong Lin - Full	SoCS	Full	X			
Hassan Khan - Assistant	SoCS	Full	X			

Davar Rezania - Associate	DOM	Full			X	X
Jamie Gruman - Full	DOM	Full	X		X	X
Louise Hayes - Associate	DOM	Full			X	
Kalinga Jagoda - Associate	DOM	Full			X	
Category 4 – Non-tenure track *core faculty members who are involved in teaching and/or supervision in other graduate program(s) in addition to being a core member of the graduate program under review.*						
Category 5 – Other core faculty*, which may include emeritus professors with supervisory privileges and other Associated Graduate Faculty members.*						
Category 6 – Special Graduate Faculty *members.*						

1. Indicate the budget unit paying the salary (department, school, research centre or institute, or other).
2. Indicate the level of supervisory privileges held by each faculty member (full, master's only, co-supervision only, etc.).
3. The program will not have identified fields of study; however, areas of expertise related to cybersecurity and management have been defined in the below table as follows: 1 = "Cybersecurity;" 2 = "Data Governance," 3 = "Management," 4 = "Leadership"

2. *Describe how instruction and supervisory loads will be distributed across the core faculty complement.*

CIS*6590 – Professional Seminar in Cybersecurity – Lead: Xiodong Lin; alternative instructor(s): Ali Dehghantanha, Rozita Dara, Hassan Khan or Charlie Obimbo.

CIS*6710 – Principles and Practice of Information Security – Lead: Hassan Khan; alternative instructor(s): Charlie Obimbo.

CIS*6720 – Cyber Security & Privacy Management and Governance – Lead: Ali Dehghantanha; alternative instructor(s): Rozita Dara, Xiaodong Lin.

BUS*6180 – Financial and Managerial Accounting – DOM Faculty or sessional instructor

BUS*6190 – Cyberpreneurship – DOM Faculty or sessional instructor

LEAD*6200 – Leadership of Organizational Change – DOM Faculty or sessional instructor

MGMT*6400 – Project Management – DOM Faculty or sessional instructor

In its first year, sessional instructors will be recruited to help deliver the courses offered as part of MCLC, with the intention of both SoCS and Lang seeking contractually-limited or tenure-track assistant professor positions as the program enrollments grow. When the program

reaches steady state, it is expected that most courses will be delivered by full-time faculty members in SoCS and Lang.

3. *Briefly comment on the areas of strength and expertise of the current core faculty complement, and note any plans for future development. Describe the ways in which—through suitable scholarly activities, professional/clinical experiences, and/or sustained participation in activities involving graduate students (e.g., seminars, colloquia, journal clubs, etc.)—the core faculty complement will foster an appropriate intellectual climate.*

Areas of faculty strength include cybersecurity, artificial intelligence and machine learning, data science, mathematical modeling and algorithms, data privacy and governance, and cryptography; as well as entrepreneurship and innovation, management, project management, organizational behaviour and leadership (see faculty CVs in Volume II).

The hiring and retention of key faculty with specific expertise in cybersecurity has been a strategic priority for SoCS in recent years. Their faculty complement includes Profs. Rozita Dara and Charlie Obimbo, as well as recent hires Ali Dehghantanha (2018), Hassan Khan (2018) and Xiaodong Lin (2019). Each of these faculty members teach at least one cybersecurity course per year.

Dr. **Ali Dehghantanha (inaugural Program Director and Graduate Program Coordinator)** is a world-leading expert in cybersecurity; a Tier 2 Canada Research Chair in Cybersecurity and Threat Intelligence; and MCTI Program Director. He has served for several years in a variety of industrial and academic positions with leading players in cybersecurity and e-Commerce. He has a long history of working in different areas of computer security as a security researcher, malware analyzer, penetration tester, security consultant, professional trainer, and university lecturer. He holds a PhD in Computer Science (Security in Computing) and a number of professional qualifications, namely CISM (Certified Information Security Manager), CCFP (Certified Cyber Forensics Professional), CISSP (Certified Information Systems Security Professional), LPT (Licensed Penetration Tester), CEH (Certified Ethical Hacker), and CHFI (Computer Hacking Forensic Investigator) (see CV in Volume II for more details). As a security researcher, he is actively investigating the latest trends in cybersecurity, digital forensics, cyber warfare, malware analysing, and exploit development.

Dr. **Rozita Dara's** research interests include: privacy and security enhancing solutions, the Internet of Things data governance and management, data mining and machine learning. She is currently pursuing several research projects in smart farming, food transparency, legal intelligence, and data governance using blockchain technology solutions. Dr. Dara is a Certified Information Privacy Technologist. She has given interviews with various media outlets, including CBC, CBC Radio-Canada, Global News, Coversation.com/Toronto.com, Guelph Mercury, SPARK (University of Guelph), Farms.com, Hill Times, Arrell Food Institute, and Canadian Poultry Magazine about the ethical and social implications of AI and automated systems, data privacy, and her research advancements. Her recent work using Twitter to track disease outbreaks was covered by the university news team, CBC and CTV News, among other outlets. The work was published in Nature's *Scientific Reports*.

Dr. **Hassan Khan** is an Assistant Professor at the University of Guelph. He received his MS and PhD from the University of Southern California and the University of Waterloo, respectively. He conducts research in Computer Security and Computer Systems domains, and he has published at prestigious venues including ACM MobiCom, ACM MobiSys, ACM CCS, and USENIX Security. Some of his research work has been featured by MSNBC, Bruce Schneier's blog, Time Magazine's Techland, The Globe and Mail, CBC, and the New Scientist magazine. His non-academic ventures include his industrial work as the Co-founder and Technical Lead at xFlow Research, where he led the development of software defined networking solutions for Marvell Technology, Netgear, Dell, and Cavium Networks. He is also a Co-founder of Penfield.AI, which is the first human-machine intelligence platform for security operations.

Prof. **Xiaodong Lin** joined SoCS in 2019. Dr. Lin received the PhD degree in Information Engineering from Beijing University of Posts and Telecommunications, China, and the PhD degree (with Outstanding Achievement in Graduate Studies Award) in Electrical and Computer Engineering from the University of Waterloo, Canada. He is currently a Professor in the SoCS, University of Guelph, Canada. His research interests include wireless communications and network security, computer forensics, software security, and applied cryptography. Dr. Lin serves on editorial board for many international journals. He has served or is serving as a guest editor for many special issues of IEEE, Elsevier and Springer journals and as a symposium chair or track chair for IEEE/ACM conferences. He also served on many program committees of international conferences. He was Chair of Communications and Information Security Technical Committee (CISTC) – IEEE Communications Society (2016-2017). He is a Fellow of the IEEE.

Dr. **Charlie Obimbo** received a Commonwealth Scholarship to do his PhD degree at the University of New Brunswick. He is currently a Professor in SoCS, which he joined after working at the University of New Brunswick and the University of Prince Edward Island. His areas of research include Computer and Network Security, where he uses AI/machine learning algorithms like support vector machines, deep learning and k-nearest neighbours to classify network payloads to help a priori detection and prevention of malicious payloads on the network. He also works in applied cryptography on blockchain technologies, and analysis and design of computer algorithms. He has designed new algorithms to solve cryptographic problems, as well as designed new ways to analyze and compare algorithm complexities. He has been a visiting professor in several universities, including United States International University-A, where he helped to establish a graduate-level Cybersecurity program.

Faculty members with research experience in related fields, as listed in Table 4, would also support the proposed program, including Dr. Andrew Hamilton-Wright.

Dr. **Andrew Hamilton-Wright** uses machine learning techniques in decision exploration systems, particularly those that leverage time-series data. He is especially interested in using rule-based association mining techniques to allow visual exploration of risk and certainty in decision making systems. Dr. Hamilton-Wright has engaged in research in diverse application areas from identification of disease classes to ergonomic data analysis. He also participates in industry-driven research, including a recent collaboration with Skyjack Inc.

After the first year, SoCS will pursue a contractually-limited faculty hire to support its cybersecurity programs, with the intention of seeking a tenure-track assistant professor position as the program popularity grows and new sections are required.

Lang faculty members who will support the design and/or delivery of MCLC curriculum components include the following:

Dr **Jamie Gruman** is a Professor of organizational behaviour, a CBE Senior Research Fellow, and serves as the Graduate Coordinator in the Organizational Leadership stream of the Ph.D. in Management. He has taught in the undergraduate program, MA Leadership Program, MBA program, and Ph.D. program in Management at the University of Guelph. In addition to being a member of numerous professional associations, Dr. Gruman is the founding Chair of the Canadian Positive Psychology Association.

Dr. **Louise Hayes** is an Assistant Professor in the Department of Management at the University of Guelph. Louise teaches accounting, audit and analytics. Her research deals with determinants of internal control and financial reporting quality. Prior to completing her PhD studies and joining the Lang School in 2014, Louise taught accounting for over twenty years at York University following seven years in public accounting where she focused on IT audit. Louise is a member of CPA Ontario and British Columbia and is a member of CPA Canada's Audit and Assurance Technology Committee.

Dr. **Davar Rezania** is Associate Professor and Chair of the Department of Management at the Lang School. Davar's research and expertise extends to project management, accountability, team leadership, sustainable economics, sustainable agriculture and bio mimicry.

Dr. **Ruben Burga** is an Assistant Professor at Lang with expertise in research and teaching in areas of Corporate Social Responsibility, project management, accountability, social entrepreneurship, and the Scholarship of Teaching and Learning.

4. *Provide evidence of adequate resources to sustain the research activities and quality of scholarship produced by students, including information technology support and laboratory access.*

The University of Guelph has made significant investments to develop and support programs in cybersecurity, including the complete overhaul of the Reynolds building, home of SoCS, and the construction of an 825-sqft cybersecurity lab that can seat up to 36 students. Moreover, the new Security Operations Centre will provide students with a state-of-the-art facility that could be used to support this program.

Students in the MCLC program will be expected to provide their own laptops. They will not require advanced computing resources such as access to servers.

We are proposing a coursework-based program. Thus, we do not require resources typically associated with thesis-based programs (e.g., student stipends). Nonetheless, the three

recently hired computer science faculty members identified above (Dehghantanha, Khan, Lin) will provide the necessary expertise required to provide leading edge scholarship in cybersecurity, including by bringing recent developments in the field into their courses and acting as supervisors to students taking CIS*6730. Practice- and sometimes knowledge-advancing research may be completed through CIS*6730, typically in association with industry partners.

Further, this program will strengthen the University's existing partnerships with some of the industry's most sophisticated security companies—Cisco Systems, IBM, Kaspersky Lab, and McAfee—who have all made substantial in-kind contributions in the form of software assets and utilities to the MCTI program and will, to varying degrees, provide access to subject matter experts, as well as real-world scenarios and datasets to support the development of case studies in the MCLC program.

Almost all MCTI industry partners have agreed to serve as long-term advisors to the proposed program; the Cybersecurity Advisory Board will be responsible for providing feedback on curriculum and other potential areas of program improvement. It is also anticipated that potential student projects for the CIS*6730 will come from the Board's membership.

5. *In **Table 6** below, summarize total operating research funds acquired by the core faculty complement over the past four (4) years. Do not include equipment grants, conference grants, or minor grants allocated by the University.*

TABLE 6. Research Funding by Source[ND2]

Year[1]	Federal Granting Councils	Other Peer Adjudicated[2]	Contracts	Others[3]
2020-21	$614,190	$531,760	0	0
2019-20	$551,500	$127,741	0	0
2018-19	$241,200	$28,154	$152,100	0
2017-18	$178,837	$63,154	0	0
Totals				

1. Record funding according to year of award start date.
2. Explain source and type in in footnote.
3. Other sources of funding include SSHRC Institutional Grants (SIG Conference, SIG-TG, SIG-GRG, SIG Exchange, and SIG Explore).

6. *Indicate whether graduate students in the proposed program will receive funding packages, and if so, the expected level and source(s) of stipend.*

This program is being proposed as a professional coursework-based master's program. Based on the logic that graduates of this type will be in high demand such that their immediate salary prospects will be quite strong, prospective students will not be extended stipends as part of their offers of admission. That said, both SoCS and Lang are committed to increasing women's access to graduate training and expect to make available special awards for outstanding

applicants from underrepresented groups in the coming admission cycles.

7. *Describe any other notable resources available to the program demonstrating institutional appropriateness (e.g., research institutes, centres, and Chairs; unique library collections or resources; facilities such as computer, laboratory, or studio spaces; etc).*

The School of Computer Science is committed to expanding its expertise and offerings in cybersecurity. It has hired several new tenure-track faculty members in the past five years, including cybersecurity and threat intelligence researchers A. Dehghantanha (2018), H. Khan (2018) and X. Lin (2019). The proposed program will dovetail with the recently launched MCTI program. The MCTI program is focused on training students in the latest tools and technologies for cybersecurity and threat intelligence whereas the proposed program is focused on training the next generation of cybersecurity management professionals and team leaders in private industry, government, and non-government organizations.

The MCTI program launched with strong support from industrial partners (BlackBerry, Cisco Systems, eSentire, Georgian Partners, IBM, ISA, McAfee Canada) including human resources and financial support. McAfee Canada (Intel) has committed a total of $1,650,337 (in-kind) between 2019–22, which includes access to all their tools, software and any required technical expertise. Moreover, eSentire, Georgian Partners, ISA, and The Co-Operators are contributing a total of $150,000 (cash) towards the funding for cybersecurity graduate students. As Dr. Dehghantanha, MCTI Program Director, played a key role in securing these industry contributions, it is expected that we will be able to leverage these resources and partnerships to benefit the proposed program. Moreover, the partners have expressed interest in shaping the curriculum, providing guest lectures, hosting internships, and providing example scenarios that will enable students to learn from real-world cybersecurity issues faced by industry.

The University has made recent investments in people and infrastructure to support cybersecurity research and training[ND3]. Besides the new faculty hires described above, the University established a Tier 2 Canada Research Chair in Cybersecurity and Threat Intelligence, which was secured by A. Dehghantanha. As part of the CRC application, the University also contributed >$75 K of its limited CFI JELF allocation for Dehghantanha's Hardware in Loop Cyberattack Simulator, enabling him to perform cyberattacks in a simulated yet close to real-world environment. The University also invested in a $2-million isolated computer lab specially designed for cybersecurity training at Guelph. It has isolated servers that enable students to emulate real-world cyberattacks without compromising the University's security.

Lang has several scholars with expertise in various areas of leadership and management. Dr. Jamie Gruman, who will teach in the MCLC program, is internationally recognized for his expertise in positive organizational behaviour and leadership. Lang recently appointed Dr. Laurie Barclay as Lang Research Chair in Leadership. Dr. Barclay is a leader in the field of leadership and organizational research and boasts an impressive research program. Although she is not initially slated to teach in the program, she will be consulted on its leadership content. Lang will be launching a Master of Project Management program in 2023. Its strength in project management will be highlighted and augmented by the launch of that program. Lang

also has significant expertise in administering graduate programs to executive and professional learners. We understand the needs and demands of such students and will apply this expertise to the recruitment and development of professional students in the MCLC program.

The University of Guelph has, in recent years, made substantial investments in people, processes, and technologies in Computing and Communications Services (CCS), thereby positioning the University to become a leader in cybersecurity best practices. Members of CCS's Information Security team have been, and will continue to be, actively involved in the design (and later in the delivery) of the MCLC program. A representative from this unit has sat on the MCTI Advisory Board. Both SoCS and Lang will work in partnership with CCS on the proposed program to share best practices in cybersecurity. Moreover, the Security Operations Centre in CCS can be used to support experiential learning opportunities; CCS personnel will provide a range of security playbooks and analyses, and provide guest talks to MCLC students about the latest threat prevention techniques.

H. Duplication, Student Demand, and Societal Need

1. *Comment on similar programs offered by other institutions in the Ontario university system and provide evidence of justifiable duplication based on demand and/or societal need.*

The proposed program is unique within the Canadian cybersecurity training landscape. While other institutions offer technical programs in cybersecurity, none provide a cross-disciplinary program that blends cybersecurity and leadership.

There are several technical cybersecurity-focused master's programs outside of the University's MCTI program. Notably, the University of Ontario Institute of Technology (UOIT) runs a Master of Information Technology Security (MITS) program—the only other graduate program in cybersecurity in Ontario, which is targeted for early-career cybersecurity technical analysts. Ryerson University and York University offer certificates in cybersecurity. Other universities in Ontario offer cybersecurity undergraduate courses (e.g., Guelph), or a stream associated with a related undergraduate degree (e.g., Carleton University), but no undergraduate programming with primary focus on cybersecurity.

In terms of national competitors, Concordia University offers a thesis-based Master of Applied Science (M.A.Sc.) with a co-op option and a Master of Engineering (M.Eng.), both in Information Systems Security.[18,19] Athabasca University offers a series of post-baccalaureate certificates and an M.Sc. in Information Systems.[20] The University of Winnipeg and the Manitoba Institute of Trade and Technology (MITT) offer a joint 13-month Network Security Diploma program that also prepares graduates for the Cisco Systems CCNA designation.[21]

[18] "Information Systems Security (MASc), Concordia University, www.concordia.ca/encs/info-systems-eng/programs/information-systems-security-masc.html.

[19] "Information Systems Security (MEng), Concordia University, www.concordia.ca/encs/info-systems-eng/programs/information-systems-security-meng.html.

[20] "Master of Science in Information Systems," Athabasca University, mscis.athabascau.ca/.

[21] "Network Security Diploma," University of Winnipeg, pace.uwinnipegcourses.ca/network-security-diploma.

Thus, there are no programs in Canada that compare to the proposed MCLC program.

There are very few comparable programs globally. There are several technical programs in cybersecurity such as an M.Sc. in Information Systems Security at Sheffield Hallam University[22]; an M.Sc. in Cyber Security, Threat Intelligence and Forensics at the University of Salford Manchester[23]; and a Master of Cyber Intelligence at the University of South Florida.[24] However, none of these programs have curricular components focused on managerial or leadership skills. To our knowledge, the only programs that blend cybersecurity and management or leadership learning outcomes include: MSc in Information Security Leadership, Brandeis University; MSc in Cyber Security Operations and Leadership, University of San Diego; Master of Cybersecurity and Leadership, University of Washington; MSc in Cybersecurity Management and Policy, University of Maryland Global Campus; and MSc in Cyber Security Leadership and Policy, Stratford University. The programs at Bradeis University and University of San Diego are completely online with limited if any experiential learning components. The University of Washington program combines principles of cybersecurity with business principles and project management courses. However, it is a 40 credit-hour program and thus assumed to be more of an overview of these concepts compared to the proposed program. The University of Maryland Global Campus program is completely online but includes a capstone course where students "assume the role of a cybersecurity professional by examining current issues in cybersecurity management." The Stratford University program includes both technical cybersecurity instruction and leadership components, but has heavy emphasis on policy development and implementation. Notably, none of these programs include curriculum components that cover topics in incident response coaching and cyberpreneurship. Thus, MCLC graduates will be uniquely positioned to lead teams in how to hunt, identify, counter, and recover from a wide range of threats within enterprise networks; as well as develop a cybersecurity startup company or lead organizational cybersecurity strategy within a startup environment.

There are some MBA programs with emphasis on cybersecurity management, such as those offered by Maryville University[25], the University of Dallas[26], and the University at Albany[27]. Moreover, there are executive programs such as Brown University's Master of Science in Cybersecurity[28], and Rutgers University's Master of Business and Science in Cybersecurity[29].

---

[22] "MSc Information Systems Security," Sheffield Hallam University, www.shu.ac.uk/study-here/find-a-course/msc-information-systems-security.

[23] "Cyber Security, Threat Intelligence and Forensics MSc," University of Salford Manchester, www.salford.ac.uk/pgt-courses/cyber-security,-threat-intelligence-and-forensics.

[24] "Master's Degree: Cyber Intelligence," University of South Florida, www.usf.edu/cybersecurity/masters-degree/cyber-intelligence.aspx.

[25] "Online Master of Business Administration in Cybersecurity," Maryville University, https://online.maryville.edu/online-masters-degrees/business-administration/concentrations/cyber-security/

[26] "The Dallas MBA," University of Dallas, https://udallas.edu/cob/academics/mba/index.php

[27] "Master of Business Administration," University at Albany, https://www.albany.edu/business/programs/mba-master-business-administration

[28] "Cybersecurity," Brown University, https://www.brown.edu/graduateprograms/cybersecurity

[29] "Cybersecurity," Rutgers University, https://mbs.rutgers.edu/academic-programs/cybersecurity

However, these programs do not have the technical depth, nor do they have any courses on data governance or cyberpreneurship, which we are proposing to cover in the MCLC program.

Finally, the University of Waterloo has announced a new Cybersecurity and Privacy Institute to build on their existing 11 undergraduate and graduate course offerings in cybersecurity and privacy. They plan to develop a diploma in cybersecurity and privacy, but no expected launch date has been identified.[30] It is expected that the proposed program and Waterloo's certificate program will have sufficiently distinct subject matter (and program duration and credentials) to attract different audiences. Regardless of when Waterloo's diploma program comes to fruition or how it is constituted, the demand for well-trained cybersecurity managers is growing at an exponential rate, justifying multiple programs of this nature within Ontario.

2. *Provide evidence of student demand for the proposed program. Consider:*
    a. *application statistics (e.g., number of inquiries, applications received, number of qualified applicants);*

    Despite not advertising this area of specialty within the current Master of Cyber Security and Threat Intelligence program, we normally receive many applications from people who do not have a technical background but who are interested in joining a course-based cybersecurity graduate program. The School regularly receives emails of interest from prospective students such as the following:

    > "I'm currently a Physics Honors student at the University of Guelph, and was looking into available programs and research on both Software Security and Encryption. I attended the CPES event last fall and was told there would potentially be a coursework-based Master's around Software Security starting in the coming years. Do you happen to have any more information on that? I see that one of the research areas is Intrusion Detection and Cryptography, I was wondering what projects you have going in that area?"

    > "I have a 3 Years Bachelor degree from Sikkim Manipal University- India and a 1 year Diploma in Computing Level-7(Networking and Server Administration) from New Zealand. I have a very deep interest in Cyber security and Networking and would be very grateful if I could pursue my further studies in University of Guelph. I am interested in the course Master of Science in Computer Science at your university. Could you please kindly look into my transcripts and let me know if I am eligible for this program or not and also let me know if I can proceed through the application process. Attached with this email is my transcripts and IELTS Score. Looking very much forward for your response. Hope you have a nice day. :)"

    The MCTI program requirements clearly indicate that applicants must have a computer science degree to meet admission requirements. However, every year, close to 20% of our applicant pool are non-technical professional applicants

[30] "Waterloo Cybersecurity and Privacy Institute: Training," University of Waterloo, uwaterloo.ca/cybersecurity-privacy-institute/training.

expressing their desire to obtain a graduate degree in cybersecurity. We believe there are many more prospective non-technical applicants who are scared away from applying when they see that a computer science degree is part of the admissions requirements. Hence, we are confident that there would be a significant applicant pool for the new MCLC program.

Cohort Year	**Total # of Applicants**	**# applicants without** a CS-related background
2020	159	14
2021 (In Progress)	168	12

Anecdotally, we received a lot of support from our industry partners interested in attending this program themselves or sending their employees. Below are example quotes from industry partners:

> "Historically, companies expected CISOs and security leaders to focus on technical deliverables. But in today's global economy, Cyber roles have drastically changed. To protect a company, Cyber Leaders need to exert strategic influence by embedding security throughout the organization and to do this well, requires leadership skills. Unfortunately, leadership skills is not something that is covered in the plethora of cybersecurity training and programs offered today." – Andrew Vezina, Vice President and CISO, EQ Bank

> "In our urgency to address the technical needs of the industry, little thought and attention has been given to who will lead this future cybersecurity workforce and bridge the gaps between the technical and business worlds of the organization. This has created a new and perhaps even more complex and challenging skills gap — one of leadership. To make progress in these areas we will need skilled cybersecurity leaders who are able to craft and implement sound strategies to hire, integrate and develop new talent. And who can also raise our profession beyond its current technical limitations, focusing simply on mitigating cyberthreats, to address the more strategic challenges of merging cybersecurity into overall business strategy, operations and culture." – Kevin Magee, Chief Security Officer, Microsoft Canada[31]

> "Increasingly, we are seeing a need to have people in cybersecurity that can speak to a variety of stakeholders within a company, from board members to different business units. This is very hard to find in the industry as some people are very strong technically, but can't translate their technical knowledge to the business." – J. Paul Haynes, President & COO, eSentire Inc.

[31] "Developing the Security Leaders we Need," Canadian Security, https://www.canadiansecuritymag.com/developing-the-security-leaders-we-need/

"Recently, BlackBerry's hiring approach has shifted from looking for the best technical talent to searching for more well-rounded individuals with stronger soft skills. We no longer look for students with the highest GPA and the strongest technical knowledge. We want someone that can perform strong on a team and be relatable with soft skills. Can perform well in a business setting." – Ryan Harkins, Vice President, BlackBerry Engineering and Operations

"I would be interested in a program like this as I did not have formal cybersecurity training. I believe a program like this can help propel my career forward and help increase my credibility in the domain of cybersecurity to my colleagues." – Director of Fusion Intelligence, CIBC

b. origin of student demand (i.e., percent domestic versus international);

The origin of expressed interest has primarily been domestic, specifically from company executives and working professionals; however, SoCS has also received inquiries from international working professionals who want to specialize in cybersecurity leadership.

c. duration of projected demand (i.e., short, medium, or long-term demand); and

It is expected that there will be long-term demand for the proposed program (i.e., >10 years). Not only is there currently a shortage of security professionals, but also the demand for qualified individuals will undoubtedly increase over time, establishing long-term demand from industry for qualified workers in this field. Christopher D. Young, President of McAfee, echoes that as security threats increase, the void of qualified professionals will persist into the foreseeable future: "We're approaching a cybersecurity talent shortage of 2 million people worldwide in the next 3 to 5 years. It's imperative that universities, private companies, and governments join forces to orient today's students toward tomorrow's cyber jobs. Every cybersecurity provider can contribute, and when we're joined by respected education institutions like the University of Guelph, our combined effort makes the world safer."

d. student consultation (e.g., student surveys, focus groups, and/or review and comment by appropriate student organization(s)).

N/A

3. *Provide evidence[32] that that the proposed program will fulfill a societal need, and indicate at least three occupations that graduates from this proposed program may be employed in. Consider:*

[32] *Examples of evidence for societal need could be:*

- *letters from a variety of potential employers of graduates who have seen the curriculum and commented upon the need for graduates within their organization and, more broadly, in their field of endeavour;*
- *professional society and/or association comments about the need for graduates based on a review of the curriculum;*

a. dimensions of the societal need for graduates (e.g., socio-cultural, economic, scientific, technological);

Cyberattacks affect industries in nearly every sector, including power and utilities, manufacturing, technology, government, transport, charities, oil and gas, business, education, finance, healthcare, telecommunications, etc.[33]

In acknowledgement of the sweeping impact cyber crime has on all industries, the federal Liberals' 2018 budget[34] commits $507.7 million over five years and $108.8 million per year for the years following to the *National Cyber Security Strategy*[35] aimed at combating cyber crime and protecting government networks. Budget 2022 proposes to provide $875.2 million over five years, beginning in 2022-23, and $238.2 million ongoing for additional measures to address the rapidly evolving cyber threat landscape.[36] Canada's recent investments in cybersecurity speak to the importance of training and retaining cybersecurity experts in order to protect the private information of Canadian citizens, to prevent Canadian businesses from incurring millions of dollars in cybercrime-related losses, and to safeguard against foreign interference in future elections.

b. geographic scope of the societal need for graduates (e.g., local, regional, national; international);

The need for cybersecurity professionals is global, including local, provincial, and national demand. This need has increased significantly in the context of the global pandemic and global shift towards remote work. The Harvey Nash / KPMG CIO Survey 2020, with over 4,200 responses from CIOs and technology executives across 83 countries, revealed that 41 percent of surveyed organizations have experienced increased incidents, mainly from spear phishing and malware attacks, since shifting to remote work.[37] Importantly, cybersecurity expertise has become the most in-demand skill set by CIOs who were surveyed.

c. trends in societal need for graduates; and

- *employment surveys indicating the number of positions advertised in, for example, the CAUT Bulletin, AUCC University Affairs, etc.;*
- *statistics related to the number of Ontario students leaving the province to study in the same field elsewhere in Canada or abroad.*

[33] "Everything Changed. Or did it?" Harvey Nash/KPMG CIO Survey 2020, https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/10/harvey-nash-kpmg-cio-survey-2020.pdf

[34] Department of Finance Canada (February 2018) Equality Growth: A Strong Middle Class, www.budget.gc.ca/2018/docs/plan/budget-2018-en.pdf.

[35] "National Cyber Security Strategy," https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

[36] Department of Finance Canada (April 2022) A Plan to Grow our Economy and Make Life More Affordable, https://budget.gc.ca/2022/pdf/budget-2022-en.pdf

[37] "Everything Changed. Or did it?" Harvey Nash/KPMG CIO Survey 2020, https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/10/harvey-nash-kpmg-cio-survey-2020.pdf

The number of unfilled cybersecurity jobs grew from one million positions in 2013 to 3.5 million in 2021.[38] Looking ahead, analysts expect the number of job opening to hold steady at 3.5 million unfilled cybersecurity jobs globally by 2025. The need for cybersecurity is not only limited to purely technical roles. The CISO position has been growing in number and influence within top global companies. Half of Fortune 500 companies had a CISO in 2016, 65 percent had a CISO in 2017, and all 500 reported having a CISO or equivalent role in 2021.[39] A recent survey of >1,000 business leaders across Europe, the US, and Asia/Pacific by IDC found that 75 percent of respondents claim the influence of the CISO has improved over the past three years.[40] Moreover, 90 percent of respondent agree that the CISO is involved in significant business innovation or change decisions. The pressing global need for well-trained graduates in cybersecurity and cybersecurity leadership is undeniable.

d. duration of the societal need (i.e., short, medium, or long-term).

There will be long-term societal need for cybersecurity professionals. A cybersecurity jobs report predicts that that there will be 3.5 million unfilled cybersecurity jobs globally by 2025, up from 1 million job openings in 2013.[38]

[38] "Cybersecurity Jobs Report: 3.5 Million Openings In 2025," Cybersecurity Ventures, https://cybersecurityventures.com/jobs/

[39] "List of Fortune 500 Chief Information Security Officers," Cybersecurity Ventures, https://cybersecurityventures.com/ciso-500/

[40] "The Modern, Connected CISO," IDC, https://www.capgemini.com/ca-en/wp-content/uploads/sites/10/2019/01/The-Modern-Connected-CISO-8.pdf

NEW GRADUATE PROGRAM PROPOSAL

VOLUME II: SUPPORTING DOCUMENTATION

A. Letters of Support
    1. CEPS Dean
    2. Lang Dean
    3. School of Computer Sciences Director
    4. OpenEd Executive Director
    5. Industry and community partners
        i. VP, Chief Information Security Officer, The Co-operators
        ii. VP, Ontario, Long View Systems
        iii. President and CEO, ISA Cybersecurity
        iv. President and COO, eSentire
        v. Executive Director, Canadian Cyber Threat Exchange
        vi. Chief Security Officer, Microsoft Canada

B. Library Assessment

C. Curriculum Documentation
    1. Learning Outcomes Alignment Template
    2. Calendar Copy
    3. Course Outlines and Course Addition/Change Forms

D. Faculty Curricula Vitae

CIS*6590
Professional Seminar in Cybersecurity

UNIVERSITY of GUELPH

1 INSTRUCTOR

Instructor: varies

Office: Reynolds

Phone extension:

E-mail:

2 AIMS & OBJECTIVES

2.1 Calendar Description

This course offers a university-wide multidisciplinary forum for discussion of topics related to Cybersecurity. The professional seminar provides an opportunity to work on different academic and industry issues related to cybersecurity at the graduate level. The intent of this course is to foster professional skills development (academic and industry); promote collaboration between industry experts and graduate students; facilitate mentoring and project development; and contribute to the transfer of knowledge between industry and university.

2.2 Course Description

This course offers a university-wide multidisciplinary forum for discussion of topics related to Cybersecurity. The professional seminar provides an opportunity to work on different academic and industry issues related to cybersecurity at the graduate level. The intent of this course is to foster professional skills development (academic and industry); promote collaboration between industry experts and graduate students; facilitate mentoring and project development; and contribute to the transfer of knowledge between industry and university. Twelve seminars a year (over 2 semesters) will be coordinated by the course instructor. The format for the seminar will include a combination of online or live workshops, guest speakers/panels, and discussions in different areas of cybersecurity, privacy, digital forensics, incident handling, etc. Subject areas discussed in any semester will depend upon the interests of students, instructor, and industry partners. This course is required for all students in the Master of Cybersecurity and Threat

Intelligence and available to graduate students from all other disciplines and collages interested in cybersecurity.

2.3 Learning Outcomes

Learning outcomes will depend on the content of seminars being offered. Generally following outcomes will be pursued:

1. Critically evaluate emerging technologies and applications in cybersecurity;
2. Integrate and communicate knowledge about emerging academic and industrial trends in cybersecurity
3. Apply gained knowledge to the development of new approaches for solving real-world cybersecurity problems.

2.4 Instructor's Role and Responsibility to Students

The role of the instructor is to facilitate presentations, discussions, and provide an environment for collaborative learning.

3 Teaching and Learning Activities

3.1 Timetable

Lectures: 3 hours per week (six weeks in Fall, six weeks in Winter)

3.2 Course Topics and Schedule

Course topic varies depending on emerging issues and concepts in cybersecurity. The course tends to focus more on researching and presenting timely topics related to cybersecurity by industry and external academic experts.

4 Learning Resources

4.1 Course Website

Course material, news, announcements, and grades will be regularly posted to the CIS*65YY Courselink site. Students are responsible for checking the site regularly.

4.2 Required Resources

Recommended resources depends on the instructor and topics being offered by external experts.

5 ASSESSMENT

5.1 Dates and Distribution

Assignment	Due Date	Weighting	Learning Outcome(s) Assessed
Research Assignment1	TBD (before the 40th class day in Fall)	50%	LO1, LO2, LO3
Research Assignment2	TBD (before the 40th class day in Winter)	50%	LO1, LO2, LO3

5.2 Assessment Descriptions

Research Assignment: Students are required to submit a research work each semester in collaboration with one or more external experts on a topic of common interest in cybersecurity.

5.3 Course Grading Policies

Accommodation of Religious Obligations: If you are unable to meet an in-course requirement due to religious obligations, please email the course instructor within two weeks of the start of the semester to make alternate arrangements. See the graduate calendar for information on regulations and procedures for Academic Accommodation of Religious Obligations: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2228.shtml

Passing grade: In order to pass the course, students must obtain a grade of 65% or higher on the total mark of all assessments.

5.4 Course Grading Policies

Accommodation of Religious Obligations: If you are unable to meet an in-course requirement due to religious obligations, please email the course instructor within two weeks of the start of the semester to make alternate arrangements. See the graduate calendar for information on regulations and procedures for Academic Accommodation of Religious Obligations: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2228.shtml

Passing grade: In order to pass the course, students must obtain a grade of 65% or higher on the total mark of all assessments.

6 University Statements

6.1 Email Communication

As per university regulations, all students are required to check their e-mail account regularly; e-mail is the official route of communication between the University and its students.

6.2 When You Cannot Meet a Course Requirement

When you find yourself unable to meet an in-course requirement because of illness or compassionate reasons please advise the course instructor (or designated person, such as a teaching assistant) in writing, with your name, id#, and e-mail contact. The grounds for Academic Consideration are detailed in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/index.shtml

6.3 Drop Date

Courses that are one semester long must be dropped by the end of the fortieth class day; two-semester courses must be dropped by the last day of the add period in the second semester. The regulations and procedures for changing graduate course registration are available in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-reg-regchg.shtml

6.4 Copies of Out-of-class Assignments

Keep paper and/or other reliable back-up copies of all out-of-class assignments; you may be asked to resubmit work at any time.

6.5 Accessibility

The University promotes the full participation of students who experience disabilities in their academic programs. To that end, the provision of academic accommodation is a shared responsibility between the University and the student.

When accommodations are needed, the student is required to first register with Student Accessibility Services (SAS). Documentation to substantiate the existence of a disability is required; however, interim accommodations may be possible while that process is underway.

Accommodations are available for both permanent and temporary disabilities. It should be noted that common illnesses such as a cold or the flu do not constitute a disability.

Use of the SAS Exam Centre requires students to book their exams at least seven days in advance and not later than the fortieth class day.

More information can be found on the SAS website: https://www.uoguelph.ca/sas

6.6 Academic Misconduct

The University of Guelph is committed to upholding the highest standards of academic integrity, and it is the responsibility of all members of the University community—faculty, staff, and students—to be aware of what constitutes academic misconduct and to do as much as possible to prevent academic offences from occurring. University of Guelph students have the responsibility of abiding by the University's

policy on academic misconduct regardless of their location of study; faculty, staff, and students have the responsibility of supporting an environment that discourages misconduct. Students need to remain aware that instructors have access to and the right to use electronic and other means of detection.

Please note: Whether or not a student intended to commit academic misconduct is not relevant for a finding of guilt. Hurried or careless submission of assignments does not excuse students from responsibility for verifying the academic integrity of their work before submitting it. Students who are in any doubt as to whether an action on their part could be construed as an academic offence should consult with a faculty member or faculty advisor.

The Academic Misconduct Policy is detailed in the Graduate Calendar:
https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2642.shtml

6.7 Recording of Materials

Presentations that are made in relation to course work—including lectures—cannot be recorded or copied without the permission of the presenter, whether the instructor, a student, or guest lecturer. Material recorded with permission is restricted to use for that course unless further permission is granted.

6.8 Resources

The Academic Calendars are the source of information about the University of Guelph's procedures, policies, and regulations that apply to undergraduate, graduate, and diploma programs:
https://www.uoguelph.ca/academics/calendars

CIS*6710 Principles and Practice of Information Security
Fall 2023

UNIVERSITY of GUELPH

1 INSTRUCTOR

Instructor:

Office:

Phone extension:

E-mail:

2 AIMS & OBJECTIVES

2.1 Calendar Description

This course teaches the foundations of cybersecurity and its applications in cyber risk assessment, identification of cyberattacks and threats, and controls for defenses and recovery. Fundamentals of cybersecurity are covered in sufficient breadth and depth so that the students can analyze systems for weaknesses, design a security policy, and identify controls that will help enforce security policies. Where applicable, real life case studies will be discussed to learn why security systems fail.

Learning Objectives

Upon successful completion of this course, students will have demonstrated the ability to:

1. Apply appropriate cybersecurity concepts for risk assessment;
2. Apply appropriate cybersecurity concepts and controls to analyse threats and protect data and systems;
3. Identify common security vulnerabilities and pitfalls in system design and suggest measures to avoid those;

4. Evaluate and interpret relevant facts, concepts, principles, and theories relating to designing and developing secure systems and use them to evaluate and improve the security of real-world systems;
5. Apply various cybersecurity standards throughout the cyber environment of a modern organization; and
6. Integrate ethics, regulations, and best practices in cybersecurity.

2.2 Instructor's Role and Responsibility to Students

The role of the instructor is to deliver lectures, facilitate discussion and provide feedback to students.

3 Teaching and Learning Activities

3.1 Timetable

Lectures: 6 hours per week

3.2 Course Topics and Schedule

Week	Topic
Week 1	Introduction, Risk and Vulnerability Assessment
Week 2	Cryptography in Practice
Week 3	Network Security
Week 4	Web Security Privacy Enhancing Technologies
Week 5	User Authentication Usable Security
Week 6	Mobile Security Cloud Security
Week 7	Managing Development of Secure Systems Cybersecurity Standards

4 Learning Resources

4.1 Course Website

Course material, news, announcements, and grades will be regularly posted to the CIS*6710 Courselink site. You are responsible for checking the site regularly.

4.2 Required Resources

1. **Computer Security and the Internet: Tools and Jewels** by Paul C. van Oorschot. 2020, Springer.
2. Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition by Ross Anderson. Available online for free.

---

5 ASSESSMENT

5.1 Dates and Distribution

Assessment	Due Date	Weighting	Learning Outcome(s) Assessed
Assignment 1	TBA	20%	LO1, LO2, LO5
Assignment 2	TBA	20%	LO3, LO4, LO5
Assignment 3	TBA	20%	LO3, LO4, LO5
Final Project	TBA	40%	LO1, LO2, LO3, LO4, LO5, LO6

5.2 Assessment Descriptions

Assignments

All assignments are to be submitted individually and electronically. Submission deadline is at 23:59 on the due date. Detailed instruction on the content of each assignment will be distributed during the term.

Final Project

Students should undertake research in the areas of security and privacy. They will identify security and privacy issues with real-world systems and apply their knowledge to develop solutions. They will communicate their findings in the form of a written report.

Projects should be done in a group of two. If students have strong reasons to do the project individually or in a larger group, they need permission from the instructor.

5.3 Course Grading Policies[NT1]

Accommodation of Religious Obligations: If you are unable to meet an in-course requirement due to religious obligations, please email the course instructor within two weeks of the start of the semester to make alternate arrangements. See the graduate calendar for information on regulations and procedures for Academic Accommodation of Religious Obligations: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2228.shtml

Passing grade: In order to pass the course, students must obtain a grade of 65% or higher on the total mark of all assessments.

6 UNIVERSITY STATEMENTS[NT2]

6.1 Email Communication

As per university regulations, all students are required to check their e-mail account regularly; e-mail is the official route of communication between the University and its students.

6.2 When You Cannot Meet a Course Requirement

When you find yourself unable to meet an in-course requirement because of illness or compassionate reasons please advise the course instructor (or designated person, such as a teaching assistant) in writing, with your name, id#, and e-mail contact. The grounds for Academic Consideration are detailed in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/index.shtml

6.3 Drop Date

Courses that are one semester long must be dropped by the end of the fortieth class day; two-semester courses must be dropped by the last day of the add period in the second semester. The regulations and procedures for changing graduate course registration are available in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-reg-regchg.shtml

6.4 Copies of Out-of-class Assignments

Keep paper and/or other reliable back-up copies of all out-of-class assignments; you may be asked to resubmit work at any time.

6.5 Accessibility

The University promotes the full participation of students who experience disabilities in their academic programs. To that end, the provision of academic accommodation is a shared responsibility between the University and the student.

When accommodations are needed, the student is required to first register with Student Accessibility Services (SAS). Documentation to substantiate the existence of a disability is required; however, interim accommodations may be possible while that process is underway.

Accommodations are available for both permanent and temporary disabilities. It should be noted that common illnesses such as a cold or the flu do not constitute a disability.

Use of the SAS Exam Centre requires students to book their exams at least seven days in advance and not later than the fortieth class day.

More information can be found on the SAS website: https://www.uoguelph.ca/sas

6.6 Academic Misconduct

The University of Guelph is committed to upholding the highest standards of academic integrity, and it is the responsibility of all members of the University community—faculty, staff, and students—to be aware of what constitutes academic misconduct and to do as much as possible to prevent academic offences from occurring. University of Guelph students have the responsibility of abiding by the University's

policy on academic misconduct regardless of their location of study; faculty, staff, and students have the responsibility of supporting an environment that discourages misconduct. Students need to remain aware that instructors have access to and the right to use electronic and other means of detection.

Please note: Whether or not a student intended to commit academic misconduct is not relevant for a finding of guilt. Hurried or careless submission of assignments does not excuse students from responsibility for verifying the academic integrity of their work before submitting it. Students who are in any doubt as to whether an action on their part could be construed as an academic offence should consult with a faculty member or faculty advisor.

The Academic Misconduct Policy is detailed in the Graduate Calendar:
https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2642.shtml

6.7 Recording of Materials

Presentations that are made in relation to course work—including lectures—cannot be recorded or copied without the permission of the presenter, whether the instructor, a student, or guest lecturer. Material recorded with permission is restricted to use for that course unless further permission is granted.

6.8 Resources

The Academic Calendars are the source of information about the University of Guelph's procedures, policies, and regulations that apply to undergraduate, graduate, and diploma programs:
https://www.uoguelph.ca/academics/calendars

CIS*6720

Cyber Security & Privacy Management and Governance

Summer Semester

UNIVERSITY of GUELPH

1 INSTRUCTOR

Instructor: Ali Dehghantanha, Rozita Dara, Xiaodong Lin

Office: REY 3319, 3311, 2210

Phone extension: 5299, 58762, 53889

E-mail: adehghan@uoguelph.ca, drozita@uoguelph.ca, xlin08@uoguelph.ca

2 AIMS & OBJECTIVES

2.1 Calendar Description

This course first offers a foundation of privacy and ethical implications of data-driven technologies, information security governance framework and supporting processes to manage information risk to an acceptable level based on the organization risk appetite and objectives. The course introduces state of the art security architecture, incident detection, containment and eradication and strategies to integrate different security technologies to achieve organization objectives. It covers an overview of privacy, ethical principles and their applications, and methods and best practices for risk mitigation, compliance and governance throughout the technology development lifecycle. It then looks at methods to build and maintain an information security program that identifies, manages and protects the organization's assets while aligning the information security strategy with the business goals to develop an effective security posture. This course is delivered on-campus in 10-day intensive teaching format.

2.2 Course Description

This course offers an overview of privacy legislation and ethical theories/principles and their applications. The course also examines strategies standards, and best practices for privacy and ethical risk assessment, mitigation. compliance, and governance. Moreover**,** the course introduces state of the art security architecture, incident detection, containment and eradication and strategies to integrate different security technologies to achieve organization objectives. In addition, it provides a comprehensive review of

information security governance framework and supporting processes to manage information risk to an acceptable level. It then looks at methods to build and maintain an information security program that identifies, manages and protects the organization's assets.

2.3 Learning Outcomes

Upon successful completion of this course, students will have demonstrated the ability to:

1. Assess security, privacy, legal and ethical risks using best practices and standardized frameworks;
2. Apply regulatory frameworks and standards for data protection and privacy to mitigate risks and enhance compliance;
3. Build and maintain an information security program that identifies, manages and protects the organization's assets;
4. Build response strategies for handling various types of cyber security incidents;
5. Establish an information security governance framework to ensure that the information security strategy is aligned with organizational goals and objectives; and
6. Manage the enterprise cyber security risks to an acceptable level based on the organization risk appetite, goals and objectives.

2.4 Instructor's Role and Responsibility to Students

The role of the instructor is to deliver lectures, facilitate discussions, provide an environment for collaborative learning, and provide feedback to students.

3 TEACHING AND LEARNING ACTIVITIES

3.1 Timetable

Lectures: 7 hours per day for total of 70 hours

Assignment project: for a total of 50 hours independent works

3.2 Course Topics and Schedule

Day	Topic
Day 1	Introduction to privacy, legal and ethical issues in managing an organization cyber security posture and Culture, Behaviour, and Security Awareness
Day 2	Introduction to data and technology development lifecycles
Day 3	Review global privacy regulations and principles and legal compliance requirements
Day 4	Processes, best practices, and standards for data protection and ethical and responsible development and use of technologies
Day 5	Privacy, ethics, and compliance enhancing technology solutions

Day 6	Information and technology governance solutions and standards
Day 7	Information Risk Identification Management and Analysis
Day 8	Information Security Program Development and Management
Day 9	Information Security Incident Management and Program Implementation
Day 10	Cyber risk quantification and Governance of Enterprise IT

4 LEARNING RESOURCES

4.1 Course Website

Course material, news, announcements, and grades will be regularly posted to the CIS*6720 Courselink site. Students are responsible for checking the site regularly.

4.2 Required Resources

- Fiona Hobbs (2017), Information Security: Procedures, Standards and Management, CRC Press, 1st Edition
- Alan Calder, Steve Watkins (2015) IT Governance: An International Guide to Data Security and ISO27001/ISO27002, Kogan Page; 6th Edition.
- J.C. Cannon. Privacy in Technology: Standards and Practices for Engineers and Security and IT Professionals. IAPP: 2014.
- Melissa Lukings and Arash Habibi Lashkari, Understanding Cybersecurity Law and Digital Privacy: A Common Law Perspective (Future of Business and Finance), Springer, 2021.

5 ASSESSMENT

5.1 Dates and Distribution

Assessment	Due Date	Weighting	Learning Outcome(s) Assessed
Assignment(s)	TBD	50%	LO1, LO2, LO3, LO5, LO6
Exam(s)/Quiz(s)	TBD	50%	LO1, LO2, LO3, LO4

1. Assess security, privacy, legal and ethical risks using best practices and standardized frameworks;
2. Apply regulatory frameworks and standards for data protection and privacy to mitigate risks and enhance compliance;

3. Build and maintain an information security program that identifies, manages and protects the organization's assets;
4. Establish an incident handling and response procedure;
5. Establish an information security governance framework to ensure that the information security strategy is aligned with organizational goals and objectives; and
6. Manage the enterprise cyber security risks to an acceptable level based on the organization risk appetite, goals and objectives.

5.2 Assessment Descriptions

Assignment(s)

Student will assess security, privacy, legal and ethical risks using best practices and standardized frameworks and apply regulatory frameworks and standards for data protection and privacy to mitigate risks and enhance compliance. In addition, students need to develop an information security program that identifies, manages and protects the organization's assets aligned with the organization information security governance framework to ensure achieving organizational goals and objectives and to manage the enterprise cyber security risks to an acceptable level.

Exam(s)/Quiz(s)

Students will be required to take several in-class quizzes on the course content. The exam(s) evaluate students capabilities in assessing security, privacy, legal and ethical risks and test their knowledge in applying regulatory frameworks and standards for data protection and privacy to mitigate risks. Students will also be evaluated on their skills to build and maintain an information security program and in establishing an incident handling and response procedure.

5.3 Course Grading Policies

Accommodation of Religious Obligations: If you are unable to meet an in-course requirement due to religious obligations, please email the course instructor within two weeks of the start of the semester to make alternate arrangements. See the graduate calendar for information on regulations and procedures for Academic Accommodation of Religious Obligations: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2228.shtml

Passing grade: In order to pass the course, students must obtain a grade of 65% or higher on the total mark of all assessments.

6 University Statements

6.1 Email Communication

As per university regulations, all students are required to check their e-mail account regularly; e-mail is the official route of communication between the University and its students.

6.2 When You Cannot Meet a Course Requirement

When you find yourself unable to meet an in-course requirement because of illness or compassionate reasons please advise the course instructor (or designated person, such as a teaching assistant) in writing, with your name, id#, and e-mail contact. The grounds for Academic Consideration are detailed in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/index.shtml

6.3 Drop Date

Courses that are one semester long must be dropped by the end of the fortieth class day; two-semester courses must be dropped by the last day of the add period in the second semester. The regulations and procedures for changing graduate course registration are available in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-reg-regchg.shtml

6.4 Copies of Out-of-class Assignments

Keep paper and/or other reliable back-up copies of all out-of-class assignments; you may be asked to resubmit work at any time.

6.5 Accessibility

The University promotes the full participation of students who experience disabilities in their academic programs. To that end, the provision of academic accommodation is a shared responsibility between the University and the student.

When accommodations are needed, the student is required to first register with Student Accessibility Services (SAS). Documentation to substantiate the existence of a disability is required; however, interim accommodations may be possible while that process is underway.

Accommodations are available for both permanent and temporary disabilities. It should be noted that common illnesses such as a cold or the flu do not constitute a disability.

Use of the SAS Exam Centre requires students to book their exams at least seven days in advance and not later than the fortieth class day.

More information can be found on the SAS website: https://www.uoguelph.ca/sas

6.6 Academic Misconduct

The University of Guelph is committed to upholding the highest standards of academic integrity, and it is the responsibility of all members of the University community—faculty, staff, and students—to be aware of what constitutes academic misconduct and to do as much as possible to prevent academic offences from occurring. University of Guelph students have the responsibility of abiding by the University's

policy on academic misconduct regardless of their location of study; faculty, staff, and students have the responsibility of supporting an environment that discourages misconduct. Students need to remain aware that instructors have access to and the right to use electronic and other means of detection.

Please note: Whether or not a student intended to commit academic misconduct is not relevant for a finding of guilt. Hurried or careless submission of assignments does not excuse students from responsibility for verifying the academic integrity of their work before submitting it. Students who are in any doubt as to whether an action on their part could be construed as an academic offence should consult with a faculty member or faculty advisor.

The Academic Misconduct Policy is detailed in the Graduate Calendar:
https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2642.shtml

6.7 Recording of Materials

Presentations that are made in relation to course work—including lectures—cannot be recorded or copied without the permission of the presenter, whether the instructor, a student, or guest lecturer. Material recorded with permission is restricted to use for that course unless further permission is granted.

6.8 Resources

The Academic Calendars are the source of information about the University of Guelph's procedures, policies, and regulations that apply to undergraduate, graduate, and diploma programs:
https://www.uoguelph.ca/academics/calendars

CIS*6730

Cybersecurity Management & Governance Project

Fall, Winter, and Summer Semesters

UNIVERSITY of GUELPH

---

1 INSTRUCTOR

Instructor: Ali Dehghantanha

Office: REY 3326

Phone extension: 52999

E-mail: adehghan@uoguelph.ca

2 AIMS & OBJECTIVES

2.1 Calendar Description

Students plan, develop, and write an industry-led research paper and produce required programs and implement controls in the industry environment. Alternatively, students may choose to work on developing a start-up business and produce a market assessment report for their products. All projects should contribute to advancing knowledge or practice and address an emerging challenge in cybersecurity, security management, security governance and incident response or a closely related field.

2.2 Course Description

Students plan, develop, and write an industry-led research paper and produce required programs and implement controls in the industry environment. Projects should contribute to advancing knowledge or practice and address an emerging challenges in cybersecurity, security management, security governance and incident response or a closely related field.

2.3 Learning Outcomes

Upon successful completion of this course, students will have demonstrated the ability to:

1. Work closely and efficiently with different industry stakeholders to identify and address a challenge in cybersecurity management and attack analysis, or a closely related field;
2. Independently manage and implement a research and development project in cybersecurity management, audit, compliance, market research or closely related field and professionally deliver the project outcome along with a research paper to the project stakeholders;
3. Critically analyse various aspects of an emerging challenge in cybersecurity governance and develop security programs to address the challenge; and
4. Analyse and integrate ethics, regulations, and best practices in planning, development, and implementation of the research project and writing of the research paper.

2.4 Instructor's Role and Responsibility to Students

The project title, summary, name of the proposed supervisor, and ethics form should be submitted to program director prior to conducting any of the project activities. The director will either approve the project or provide the student with detailed feedback and directions to revise and resubmit the proposal.

Once a project is approved, a faculty member as project mentor will work closely with the project team (student and industry advisor) and provide timely feedback and evaluation. The project team will submit the project proposal, project solution, and final project paper to the mentor. All project deliverables are evaluated by the project mentor (as described in Assessment section, below) and all project marks are submitted to the program director for final approval.

3 TEACHING AND LEARNING ACTIVITIES

3.1 Course Schedule

Students are required to identify an industry or an academic expert who is willing to support their project. Students are strongly encouraged to begin looking for an industry or academic expert to partner within the first (Fall) semester of the program.

Date	Activity
January	Student liaises with prospective supervisor, prospective mentor, and course instructor to develop project concept and complete ethics form
February 1	Submission of project title, summary, name of supervisor, and ethics form to the program director
February 15	Project approval from the project director and project kick-off
March 15	Submission of the **project proposal** to the project mentor
April 1	Feedback on the project proposal by the project mentor
July 15	**Project solution** presentation and delivery to the project mentor
August 1	Feedback on the project solution by the project mentor
August 15	Submission of project **final paper** and all deliverables to the project mentor
August 31	Final paper feedback of evaluation by the project mentor

4 LEARNING RESOURCES

4.1 Course Website

Standard rubrics for the evaluation of student work will be posted to the CIS*6730 Courselink site. Students, mentors, and supervisors will all have access to the rubrics throughout the course.

5 ASSESSMENT

5.1 Dates and Distribution

Assessment	Due Date	Weighting	Learning Outcome(s) Assessed
Project Proposal	March 15	20%	LO1, LO3, LO4
Project Solution	July 15	40%	LO1, LO3, LO4
Final Paper (and other deliverables)	August 15	40%	LO1, LO2, LO3, LO4

5.2 Assessment Descriptions

Project Proposal

The project proposal should clearly define the research gap, state the problem, and the project approach/methodology. The project proposal will be evaluated by the faculty project mentor according to a standardized rubric provided by the program director.

Project Solution

The project solution should include any tools, software, or services that address the research gap along with rigorous evaluation of project results and identification of any challenges or limitation for the project. The project solution will be evaluated by the project supervisor according to a standardized rubric provided by the program director.

Final Paper and Other Project Deliverables

The final paper is a rigorous academic or industry report, following standard writing and formatting requirements of major publications in the field. The project paper should clearly explain the project gap, the problem, project methodology/approach, proposed solution, evaluation, and analysis of the results, and offer a conclusion and discussion of future works. All project deliverables are evaluated by the project mentor, according to a standardized rubric provided by the program director, and all project marks are submitted to the Cybersecurity Project Committee for final approval.

Students will receive a SAT or UNSAT notation upon completion of this course.

5.3 Course Grading Policies

Accommodation of Religious Obligations: If you are unable to meet an in-course requirement due to religious obligations, please email the course instructor within two weeks of the start of the semester to make alternate arrangements. See the graduate calendar for information on regulations and procedures for Academic Accommodation of Religious Obligations: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2228.shtml

Passing grade: In order to pass the course, students must obtain a grade of 65% or higher on the total mark of all assessments.

---

6 University Statements

6.1 Email Communication

As per university regulations, all students are required to check their e-mail account regularly; e-mail is the official route of communication between the University and its students.

6.2 When You Cannot Meet a Course Requirement

When you find yourself unable to meet an in-course requirement because of illness or compassionate reasons please advise the course instructor (or designated person, such as a teaching assistant) in writing, with your name, id#, and e-mail contact. The grounds for Academic Consideration are detailed in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/index.shtml

6.3 Drop Date

Courses that are one semester long must be dropped by the end of the fortieth class day; two-semester courses must be dropped by the last day of the add period in the second semester. The regulations and procedures for changing graduate course registration are available in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-reg-regchg.shtml

6.4 Copies of Out-of-class Assignments

Keep paper and/or other reliable back-up copies of all out-of-class assignments; you may be asked to resubmit work at any time.

6.5 Accessibility

The University promotes the full participation of students who experience disabilities in their academic programs. To that end, the provision of academic accommodation is a shared responsibility between the University and the student.

When accommodations are needed, the student is required to first register with Student Accessibility Services (SAS). Documentation to substantiate the existence of a disability is required; however, interim accommodations may be possible while that process is underway.

Accommodations are available for both permanent and temporary disabilities. It should be noted that common illnesses such as a cold or the flu do not constitute a disability.

Use of the SAS Exam Centre requires students to book their exams at least seven days in advance and not later than the fortieth class day.

More information can be found on the SAS website: https://www.uoguelph.ca/sas

6.6 Academic Misconduct

The University of Guelph is committed to upholding the highest standards of academic integrity, and it is the responsibility of all members of the University community—faculty, staff, and students—to be aware of what constitutes academic misconduct and to do as much as possible to prevent academic offences from occurring. University of Guelph students have the responsibility of abiding by the University's policy on academic misconduct regardless of their location of study; faculty, staff, and students have the responsibility of supporting an environment that discourages misconduct. Students need to remain aware that instructors have access to and the right to use electronic and other means of detection.

Please note: Whether or not a student intended to commit academic misconduct is not relevant for a finding of guilt. Hurried or careless submission of assignments does not excuse students from responsibility for verifying the academic integrity of their work before submitting it. Students who are in any doubt as to whether an action on their part could be construed as an academic offence should consult with a faculty member or faculty advisor.

The Academic Misconduct Policy is detailed in the Graduate Calendar:
https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2642.shtml

6.7 Recording of Materials

Presentations that are made in relation to course work—including lectures—cannot be recorded or copied without the permission of the presenter, whether the instructor, a student, or guest lecturer. Material recorded with permission is restricted to use for that course unless further permission is granted.

6.8 Resources

The Academic Calendars are the source of information about the University of Guelph's procedures, policies, and regulations that apply to undergraduate, graduate, and diploma programs:
https://www.uoguelph.ca/academics/calendars

MGMTxxxx Cyberpreneurship

Winter/Fall 2022

Cohort: …

Credit Weight: 0.50

Course Details

Calendar Description

This course merges the disciplines of entrepreneurship and cybersecurity with a focus on the process of generating and launching new cybersecurity sensitive or dependent ventures. Students who successfully complete this course will be able to assess cybersecurity market opportunities, develop a startup plan, assess risks and ethical considerations and effectively communicate ideas to ensure success of new ventures.

Pre-Requisite(s):

Co-Requisite(s):

Restriction(s): Masters of Cybersecurity Leadership and Cyberpreneurship and Lang Graduate students only

Method of Delivery: Distance Education

Course Website Access Date:

Course Start Date:

Course End Date:

Final Exam

There is no final exam in this course.

Instructional Support

Instructor

Dr. Ruben Burga

Email: rburga@uoguelph.ca
Telephone: (519) 824-4120 Ext. 54463
Office: MAC Rm:222

[Instructor biography]

Office Hours via **[Zoom** [s1]**or Microsoft Teams**[s2]**]:** Students may opt to drop in to office hours on [day] from [time] to [time] beginning on [date]. Please note that further details will be posted in the **Announcements**. See also **Communicating with Your Instructor.**

Teaching Assistant(s)

Name:
Email:

Program Contact

Learning Resources

Required Textbook

Title: Business Model Generation
Author(s): Osterwalder, A. & Pigneur, Y.
Edition / Year:
Publisher: John Wiley & Sons
ISBN: 978-0470-87641-1

You may purchase the textbook at the Guelph Campus Co-op Bookstore or the University of Guelph Bookstore.

https://guelphcampus.coop/bookstore

http://www.bookstore.uoguelph.ca/

Course Materials

There are no required materials for this course.

Supplementary Materials

This course includes supplementary materials. These materials are meant to supplement the required readings and course content. You can explore the materials at your own pace. To access these materials, select **Content** on the navbar to locate **Supplementary Materials** in the table of contents panel.

The supplementary materials may be added throughout the semester depending on cases that are examined, and specific theories or practices addressed.

Course Website

CourseLink (powered by D2L's Brightspace) is the course website and will act as your classroom. It is recommended that you log in to your course website every day to check for announcements, access course materials, and review the weekly schedule and assignment requirements.

https://courselink.uoguelph.ca/

Ares

For this course, you may be required to access course reserve materials through the University of Guelph McLaughlin Library. To access these items, select **Ares** on the navbar in CourseLink. Note that you will need your Central Login ID and password in order to access items on reserve.

For further instructions on accessing reserve resources, visit How to Get Course Reserve Materials[s3].

If at any point during the course you have difficulty accessing reserve materials, please contact the e-Learning Operations and Reserve Services staff at:

Tel: 519-824-4120 ext. 53621
Email: libres2@uoguelph.ca
Location: McLaughlin Library, First Floor, University of Guelph

https://www.lib.uoguelph.ca/find/course-reserves-ares

Learning Outcomes

Course Learning Outcomes

This course provides students an opportunity to examine contemporary issues in cyberpreneurship. The course involves applying the technical, management, marketing, and financial aspects of entrepreneurship in order to integrate a perspective from the cybersecurity domain to entrepreneurial initiatives. Topics relating to the wide spectrum of technological innovations will be examined from a business viewpoint. A case-based

approach will be used to integrate both the cybersecurity and business perspective in decision-making. Relevant topics including cyberspace innovations, sustainability, and cyberpreneurship business model generation will be explored. Additional topics will vary according to the cases used.

By the end of this course, you should be able to:

1. Assess cybersecurity solutions with respect to their sustainability including technical, market and financial feasibility;
2. Develop business models and manage projects under high uncertainty;
3. Understand and utilize key skills related to entrepreneurship, relationship building, organizational change, as well as project and personnel management in the context of cyberpreneurship;
4. Develop a strategy to lead and promote change within an organization;
5. Implement communication skills related to change management in the context of cyberpreneurship (i.e., report writing, oral and written presentations);
6. Identify potential weak points that could undermine a change effort, and address sources of resistance to change;
7. Critically analyze new information regarding change using case study methodology; and
8. Understand the theory, processes and the analytical tools that can assist in the innovation and commercialization process and how best to prepare technologies to survive commercialization.

Teaching and Learning Activities

Method of Learning[MP4]

Distance education – online asynchronous learning with some synchronous elements throughout the course

Course Structure[MP5]

This course is very interactive and will require active participation of students in the weekly lectures. The Weekly Activity list may change from time to time based on class interaction. This will be noted and updated through Courselink as necessary.

Furthermore, our general approach is to create a learning environment through the use of cases, discussions, and experiential activities, where students can interact with the instructor, each other, and course material to explore and discuss management and organizational related issues to generate ideas and solutions both in class and on the course website. We believe that learning occurs when there is value creation and when

exploration into the course concepts and ideas generate the need to ask questions and challenge assumptions. We expect students to engage in the learning and discuss topics and issues through critical analysis and use multiple perspectives in the exploration of the course concepts. To enhance learning and application, students are expected to go beyond the course material and integrate knowledge from events in the media and other related and relevant resources.

What to Expect for Each Unit[MP6]

Each unit will require students to have completed the readings provided before the start of the unit; the students will discuss the readings, applicable theories and practices as part of their weekly activities using the Discussion Forum in CourseLink; the students will also participate in case analysis work to reinforce concepts from each unit.

Every unit will have a recorded guest speaker interview that is relevant to the specific week's topic. Guest speaker will be selected from the cybersecurity and cybertrepreneurship domains.

In addition to the discussion forums, there will be assessments throughout the course based on a simulated cybertrepreneurship case. Details for these assessments and specific cases will be described in Week 1.

Every unit will scaffold to prepare the students for a final recorded presentation and report oriented around commercialization or management challenges in cyberpreneurship. Depending on availability students may work on actual client opportunities or in simulated cases.

Schedule[s7]

It is strongly recommended that you follow the course schedule provided below. The schedule outlines what you should be working on each week of the course and lists the important due dates for the assessments. By following the schedule, you will be better prepared to complete the assessments and succeed in this course.

Unit 01:

Weeks 1 – Cyberpreneurship and Innovation Theories and Design Thinking practices

Readings

- Selected chapters from *Business Model Generation* textbook.
- Porter, M.E., & Heppelmann, J.E. (2014). How smart connected products are transforming competition. Harvard Business Review, 92(11). 64-88.
- Zaheer, H., Breyer, Y., & Dumay, J. (2019). Digital entrepreneurship: An interdisciplinary structured literature review and research agenda. Technological Forecasting and Social Change, 148(Complete). https://doi.org/10.1016/j.techfore.2019.119735

- Selected relevant readings from ISACA Journal (https://www.isaca.org/resources/isaca-journal) or (ISC)^2 (https://www.isc2.org/Research) [readings will change from semester to semester to remain current]

Activities

- Familiarize yourself with the course website by selecting **Start Here** on the navbar.
- Review **Outline** and **Assessments** on the course website to learn about course expectations, assessments, and due dates.
- Confirm your access to the course reserve materials by selecting **Ares** on the navbar.
- Description of Case analysis assessments and final oral recorded presentations and final report.

Assessments

- Assessment 1 (sample non-graded), Assessment 2 (sample non-graded)

Unit 02:

Weeks 2– Cyberpreneurial and Entrepreneurial Business Models

Readings

- Selected chapters from *Business Model Generation* textbook
- Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. Communications of the Association for information systems, 12(1), 50.
- Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. Decision sciences, 39(2), 273-315.
- Zenebe, A., Alsaaty, F. M., & Anyiwo, D. (2018). Relationship between individual's entrepreneurship intention, and adoption and knowledge of information technology and its applications: an empirical study. Journal of Small Business & Entrepreneurship, 30(3), 215–232. https://doi.org/10.1080/08276331.2017.1397441
- Selected relevant readings from ISACA Journal (https://www.isaca.org/resources/isaca-journal) or (ISC)^2 (https://www.isc2.org/Research) [readings will change from semester to semester to remain current]

Activities

- Guest speaker (recorded)
- Individual peer evaluations of student presentations
- Case analysis and recording of group presentations

Assessments

- Assessment 1, Assessment 2

Unit 03:

Weeks 3 – Commercialization, Innovation and Management techniques

Readings

- Selected chapters from *Business Model Generation* textbook
- Aarikka-Stenroos, L., & Lehtimäki, T. (2014). Commercializing a radical innovation: Probing the way to the market. Industrial Marketing Management, 43(8), 1372-1384
- Selected relevant readings from ISACA Journal (https://www.isaca.org/resources/isaca-journal) or $(ISC)^2$ (https://www.isc2.org/Research) [readings will change from semester to semester to remain current]

- Guest speaker (recorded)
- Individual peer evaluations of student presentations
- Case analysis and recording of group presentations

Assessments

- Assessment 1, Assessment 2

Unit 04:

Weeks 4 – Innovation, Commercialization and Financial Aspects of Cyberpreneurship

Readings

- Selected chapters from *Business Model Generation* textbook Qin, J., van der Rhee, B., Venkataraman, V., & Ahmadi, T. (2021). The impact of IT infrastructure capability on NPD performance: The roles of market knowledge and innovation process formality. *Journal of Business Research*, *133*, 252-264.

- Elia, G., Margherita, A., & Passiante, G. (2020). Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process. Technological Forecasting and Social Change, 150(Complete). https://doi.org/10.1016/j.techfore.2019.119791
- Selected relevant readings from ISACA Journal (https://www.isaca.org/resources/isaca-journal) or (ISC)^2 (https://www.isc2.org/Research) [readings will change from semester to semester to remain current]

Activities

- Guest speaker (recorded)
- Individual peer evaluations of student presentations
- Case analysis and recording of group presentations

Assessments

- Assessment 1, Assessment 2

Unit 05:

Weeks 5 – Exploring the Cyberpreneurship Ecosystem and Open Innovation concepts

Readings

- Selected chapters from *Business Model Generation* textbook Marullo, C., Casprini, E., Di Minin, A., & Piccaluga, A. (2018). 'Ready for Take-off': How Open Innovation influences startup success. Creativity and Innovation Management, 27(4), 476-488.
- Adner, R., & Kapoor, R. (2016). Innovation ecosystems and the pace of substitution: Re-examining technology S-curves. Strategic management journal, 37(4), 625-648.
- Lilli, E. (2021). Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence. Contemporary Security Policy, 42(2), 163–188. https://doi.org/10.1080/13523260.2021.1882812
- Selected relevant readings from ISACA Journal (https://www.isaca.org/resources/isaca-journal) or (ISC)^2 (https://www.isc2.org/Research) [readings will change from semester to semester to remain current]

Activities

- Guest speaker (recorded)
- Individual peer evaluations of student presentations

- Case analysis and recording of group presentations

Assessments

- Assessment 1, Assessment 2

Unit 06:

Weeks 6 – Practical Tools and Techniques to Pitch and Business Plan Development

Readings

- Selected chapters from *Business Model Generation* textbook Selected relevant readings from ISACA Journal (https://www.isaca.org/resources/isaca-journal) or $(ISC)^2$ (https://www.isc2.org/Research) [readings will change from semester to semester to remain current]
- Innovation Toolkit Courselink Access (resourced from the Wood Centre – unit linked to pitch and presentations)

Activities

- Guest speaker (recorded)
- Individual peer evaluations of student presentations
- Case analysis and recording of group presentations

Assessments

- Assessment 1, Assessment 2

Unit 07:

Week 7 – Presentation of Cyberpreneurship Cases/Proposals by Student Teams

Readings

- Selected chapters from *Business Model Generation* textbook

Activities

- Presentations and Peer evaluations of student presentations .

Assessments

- Assessment 3

Assessments

The grade determination for this course is indicated in the following table. A brief description of each assessment is provided below. Select **Content** on the navbar to locate **Assessments** in the table of contents panel to review further details of each assessment. Due dates can be found under the Schedule heading of this outline.

Table 1: Course Assessments

Assessment Item	**Weight**	**Learning Outcomes**[MP8]
Assessment 1a - Presentation of a unit content (to be recorded and posted for peer evaluations)	12	LO 1, LO 3, LO 5, LO 8
Assessment 1b - Peer Assessment of Presentations	20	LO 1, LO 3, LO 6
Assessment 2 - Case Analysis	35	LO 1, LO 2, LO 3, LO 6, LO 7
Assessment 3a - Written cyberpreneurial business plan	20	LO 2, LO 4, LO 5, LO 8
Assessment 3b - Oral recorded cyberpreneurial pitch[SL9] and funding	13	LO 2, LO 4, LO 5, LO 8
Total	**100%**	

Assessment Descriptions

Assessment 1

Assessment 1a - Every student will present that unit's content to the class as a 10-20-minute presentation based on the readings for the unit. This presentation will be recorded and posted through Courselink. Each presenting student will have three random students provide peer assessments. The structure of the presentation will be described in Week 1. The student presenter will be graded at 4%/week which will result in 20% of their total grade for these weekly presentations.

Assessment 1b- Each student will also provide an individual peer assessment of a presenter. This assessment will guide the instructor grading of the presenter and can be

viewed as anonymous ratings from the assessors. Students will be graded on the quality of their constructive assessments at 2.5% per week for a total of 12% in the term. Note that each week, every student is expected to provide one assessment and one presentation.

Assessment 2

Assessment 2 - Students will be placed in groups and will analyze a real-life cyberpreneurial case study relevant to the unit's content. Every group is expected to meet synchronously or use asynchronous tools to contribute to their group work. A final presentation will be recorded and submitted. Note that the presentation can be presented by a single group member, shared, or edited to include all members. There is no expectations that all members of the group should be present when recording their presentation. They will be graded by the instructor based on their analysis of the case, presentation of the situation, and using case analysis methods to provide suitable alternatives for the entrepreneurial/commercialization or management problems that are the focus for the week (each group member will be graded equally at 7% per presentation).

Assessment 3

Assessment 3a - Students will individually develop a written business plan for an cyberpreneurial business/product/service idea. This business plan will form the basis for their recorded oral pitch in 3b. The submission of this written business plan incorporating the material learned throughout the course is expected in Week 12 and will form 20% of their grade.

Assessment 3b - Students will do a minimum 10 minute pitch for their cyberpreneurial idea; based on a 'Dragon's Den' or 'Shark Tank' format to request funding for their entrepreneurial idea. This pitch, based on their written proposal in 3a will form 13% of their final grade as follow: 10% of the grades will be for the pitch presentation and 3% of the grade will be for participating in funding the pitches as peer evaluators. The pitch will be submitted through Courselink and will be funded by the other students in the class using artificial money. The best funded pitch as determined by the class will combine with the instructor assessment to generate the grade.

Course Technology Requirements and Technical Support

CourseLink System Requirements

You are responsible for ensuring that your computer system meets the necessary system requirements. Use the browser check tool to ensure your browser settings are compatible and up to date. (Results will be displayed in a new browser window).

https://opened.uoguelph.ca/student-resources/system-and-software-requirements[SJ10]

https://courselink.uoguelph.ca/d2l/systemCheck

[Tool Name] Requirements[VK11][s12]

Microsoft Teams System Requirements[s13]

This course may use **Microsoft Teams** as a video communication tool. A Webcam, a microphone, and headphones/speakers are also needed. In order to use **Microsoft Teams**, you must meet the following technical requirements:

1. An internet connection – broadband wired or wireless (3G or 4G/LTE);
2. Speakers and a microphone – built-in or USB plug-in or wireless Bluetooth;
3. A webcam or HD webcam - built-in or USB plug-in;
4. Supported mobile platforms: Android 4.4 or later and iOS 10.0 or later.

Technical Skills

As part of your online experience, you are expected to use a variety of technology[MP14] as part of your learning:

- Manage files and folders on your computer (e.g., save, name, copy, backup, rename, delete, and check properties);
- Install software, security, and virus protection;
- Use office applications (e.g., Word, PowerPoint, Excel, or similar) to create documents;
- Be comfortable uploading and downloading saved files;
- Communicate using email (e.g., create, receive, reply, print, send, download, and open attachments);
- Navigate the CourseLink learning environment and use the essential tools, such as **Dropbox**, **Quizzes**, **Discussions**, and **Grades** (the instructions for this are given in your course);
- Access, navigate, and search the Internet using a web browser (e.g., Firefox, Internet Explorer); and
- Perform online research using various search engines (e.g., Google) and library databases.

Technical Support

If you need any assistance with the software tools or the CourseLink website, contact CourseLink Support.

CourseLink Support
University of Guelph
Day Hall, Room 211

Email: courselink@uoguelph.ca
Tel: 519-824-4120 ext. 56939
Toll-Free (CAN/USA): 1-866-275-1478

Walk-In Hours (Eastern Time):
Monday thru Friday: 8:30 am–4:30 pm

Phone/Email Hours (Eastern Time):
Monday thru Friday: 8:30 am–8:30 pm
Saturday: 10:00 am–4:00 pm
Sunday: 12:00 pm–6:00 pm

Course Specific Standard Statements

Acceptable Use

The University of Guelph has an Acceptable Use Policy, which you are expected to adhere to.

https://www.uoguelph.ca/ccs/infosec/aup

Communicating [MP15]with Your Instructor

During the course, your instructor will interact with you on various course matters on the course website using the following ways of communication:

- **Announcements:** The instructor will use **Announcements** on the Course Home page to provide you with course reminders and updates. Please check this section frequently for course updates from your instructor.
- **Ask Your Instructor Discussion:** Use this discussion forum to ask questions of your instructor about content or course-related issues with which you are unfamiliar. If you encounter difficulties, the instructor is here to help you. Please post general course-related questions to the discussion forum so that all students have an opportunity to review the response. To access this discussion forum, select **Discussions** from the **Tools** dropdown menu.
- **Email:** If you have a conflict that prevents you from completing course requirements, or have a question concerning a personal matter, you can send your instructor a private message by email. The instructor will respond to your email within 48 to 72 hours.
- **Online meeting:** If you have a complex question you would like to discuss with your instructor, you may book an online meeting. Online meetings depend on the availability of you and the instructor, and are booked on a first come first served basis.

Netiquette Expectations

For distance education courses, the course website is considered the classroom and the same protections, expectations, guidelines, and regulations used in face-to-face settings apply, plus other policies and considerations that come into play specifically because these courses are online.

Inappropriate online behaviour will not be tolerated. Examples of inappropriate online behaviour include:

- Posting inflammatory messages about your instructor or fellow students;
- Using obscene or offensive language online;
- Copying or presenting someone else's work as your own;
- Adapting information from the Internet without using proper citations or references;
- Buying or selling term papers or assignments;
- Posting or selling course materials to course notes websites;
- Having someone else complete your quiz or completing a quiz for/with another student;
- Stating false claims about lost quiz answers or other assignment submissions;
- Threatening or harassing a student or instructor online;
- Discriminating against fellow students, instructors, and/or TAs;
- Using the course website to promote profit-driven products or services;
- Attempting to compromise the security or functionality of the learning management system;
- Sharing your username and password; and
- Recording lectures without the permission of the instructor.

Submission of Assignments to Dropbox[MP16]

All assignments for this course should be submitted electronically via the online **Dropbox** tool. When submitting your assignments using the **Dropbox** tool, do not leave the page until your assignment has successfully uploaded. To verify that your submission was complete, you can view the submission history immediately after the upload to see which files uploaded successfully. The system will also email you a receipt. Save this email receipt as proof of submission.

Be sure to keep a back-up copy of all of your assignments in the event that they are lost in transition. In order to avoid any last-minute computer problems, your instructor strongly recommend you save your assignments to a cloud-based file storage (e.g., Google Docs), or send to your email account, so that should something happen to your computer, the assignment could still be submitted on time or re-submitted.

It is your responsibility to submit your assignments on time as specified on the Schedule. Be sure to check the technical requirements and make sure you have the proper computer, that you have a supported browser, and that you have reliable Internet access. Remember that **technical difficulty is not an excuse not to turn in your assignment on time.** Don't wait until the last minute as you may get behind in your work.

If, for some reason, you have a technical difficulty when submitting your assignment electronically, please contact your instructor or CourseLink Support.

https://support.opened.uoguelph.ca/contact[SJ17]

Late Policy[MP18]

If you choose to submit your individual assignments to the **Dropbox** tool late, the full allocated mark will be reduced by 5% per day after the deadline for the submission of the assignment to a limit of six days at which time access to the **Dropbox** folder will be closed.

For late final exam submissions to the **Quizzes** tool[MP19], your attempt will be flagged as late, and you will be prevented from making further changes to your attempt once your time ends. Make sure you save all your responses to the exam questions. The **Quizzes** tool counts down your time in the upper-left hand corner. Please pay close attention to this countdown and save your answers frequently.

Extensions will be considered for medical reasons or other extenuating circumstances. If you require an extension, discuss this with the instructor as soon as possible and well before the due date. Barring exceptional circumstances, extensions will not be granted once the due date has passed. These rules are not designed to be arbitrary, nor are they inflexible. They are designed to keep you organized, to ensure that all students have the same amount of time to work on assignments, and to help to return marked materials to you in the shortest possible time.

Obtaining Grades and Feedback[MP20]

Unofficial assessment marks will be available in the **Grades** tool of the course website.

Your instructor will have grades posted online within 2 weeks of the submission deadline, if the assignment was submitted on time. Once your assignments are marked you can view your grades on the course website by selecting **Grades** from the **Tools** dropdown menu on the navbar. Your course will remain open to you for one year following the end of your program[s21].

Final grades will be available at the end of the semester. Students can access their final grade by logging into WebAdvisor (using your U of G central ID).

https://webadvisor.uoguelph.ca

Rights and Responsibilities When Learning Online

The course website is considered the classroom and the same protections, expectations, guidelines, and regulations used in face-to-face settings apply, plus other policies and considerations that come into play specifically because these courses are online.

For more information on your rights and responsibilities when learning in the online environment, visit Rights and Responsibilities.

http://opened.uoguelph.ca/student-resources/rights-and-responsibilities

Turnitin Originality Check[MP22]

In this course, your instructor will be using Turnitin, integrated with the CourseLink **Dropbox** tool, to detect possible plagiarism, unauthorized collaboration or copying as part of the ongoing efforts to maintain academic integrity at the University of Guelph.

All individual assignments submitted to the **Dropbox** tool will be included as source documents in the Turnitin.com reference database solely for the purpose of detecting plagiarism of such papers. Use of the Turnitin.com service is subject to the Usage Policy posted on the Turnitin.com site.

A major benefit of using Turnitin is that you will be able to educate and empower yourself in preventing academic misconduct. In this course, you may screen your own assignments through Turnitin as many times as you wish before the due date. You will be able to see and print reports that show you exactly where you have properly and improperly referenced the outside sources and materials in your assignment.

Program Specific Standard Statements

Equity, Diversity, and Inclusion

At the Lang School of Business and Economics, we are committed to developing leaders with a social conscience, an environmental sensibility, and a commitment to their communities. A core tenet within this vision is that diversity is a strength with which we can experience greater connection and understanding.

As such, we affirm the importance and shared responsibility of our students, faculty, and staff creating and promoting equity and inclusion within our learning spaces. Creating these kinds of learning cultures is a process, not a destination; it requires ongoing willingness on the part of each person to thoughtfully and critically listen, unlearn, learn, and engage as they are exposed to a multitude of perspectives and lived experiences. We encourage dialogues between students and instructors to address and advance opportunities for fostering greater diversity and inclusion in the learning environment. Openness to conversations with each other enables us to reflect and grow as we learn from one another respectfully and holistically.

As a department that is training the professionals of the future, we expect our learning spaces to abide by all institutional policies and guidelines, in particular those outlined by

the Office of Diversity and Human Rights and the University of Guelph Human Rights Policy. Discrimination and harassment, as defined by our policies, will not be tolerated. Individuals should inform the appropriate party as per University policies if they experience any such behaviours.

https://www.uoguelph.ca/diversity-human-rights/human-rights-policy-and-procedures

---

University Standard Statements

University of Guelph: Graduate Policies

As a student of the University of Guelph, it is important for you to understand your rights and responsibilities and the academic rules and regulations that you must abide by. Consult the Graduate Calendar for the rules, regulations, curricula, programs and fees for current and previous academic years.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Email Communication

As per university regulations, all students are required to check their uoguelph.ca e-mail account regularly: e-mail is the official route of communication between the University and its students.

When You Cannot Meet Course Requirements

When you find yourself unable to meet an in-course requirement due to illness or compassionate reasons, please advise your course instructor (or designated person such as a teaching assistant) **in writing**, with your name, ID number and email contact.

Review the Graduate Calendar for information on regulations and procedures for Academic Consideration.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Drop Date

The last date to drop one-semester courses, without academic penalty, is indicated in the Schedule of Dates section of the Graduate Calendar. Review the Graduate Calendar for regulations and procedures for Dropping Courses.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Copies of Out-of-Class Assignments

Keep paper and/or other reliable back-up copies of all assignments: you may be asked to resubmit work at any time.

Accessibility

The University promotes the full participation of students who experience disabilities in their academic programs. To that end, the provision of academic accommodation is a shared responsibility between the University and the student.

When accommodations are needed, the student is required to first register with Student Accessibility Services (SAS). Documentation to substantiate the existence of a disability is required, however, interim accommodations may be possible while that process is underway.

Accommodations are available for both permanent and temporary disabilities. It should be noted that common illnesses such as a cold or the flu do not constitute a disability.

Use of the SAS Exam Centre requires students to make a booking at least 14 days in advance, and no later than November 1 (fall), March 1 (winter) or July 1 (summer). Similarly, new or changed accommodations for online quizzes, tests and exams must be approved at least a week ahead of time.

More information: www.uoguelph.ca/sas

Academic Misconduct

The University of Guelph is committed to upholding the highest standards of academic integrity and it is the responsibility of all members of the University community – faculty, staff, and students – to be aware of what constitutes academic misconduct and to do as much as possible to prevent academic offences from occurring. University of Guelph students have the responsibility of abiding by the University's policy on academic misconduct regardless of their location of study; faculty, staff and students have the responsibility of supporting an environment that discourages misconduct. Students need to remain aware that instructors have access to and the right to use electronic and other means of detection.

The Academic Misconduct Policy is detailed in the Graduate Calendar.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Copyright

Content within this course is copyright protected. Third party copyrighted materials (such as book chapters and articles) have either been licensed for use in this course, or have been copied under an exception or limitation in Canadian Copyright law.

The fair dealing exemption in Canada's Copyright Act permits students to reproduce short excerpts from copyright-protected materials for purposes such as research, education, private study, criticism and review, with proper attribution. Any other copying, communicating, or distribution of any content provided in this course, except as permitted by law, may be an infringement of copyright if done without proper license or the consent of the copyright owner. Examples of infringing uses of copyrighted works would include uploading materials to a commercial third party web site, or making paper

or electronic reproductions of all, or a substantial part, of works such as textbooks for commercial purposes.

Students who upload to CourseLink copyrighted materials such as book chapters, journal articles, or materials taken from the Internet, must ensure that they comply with Canadian Copyright law or with the terms of the University's electronic resource licenses.

For more information about students' rights and obligations with respect to copyrighted works, review Fair Dealing Guidance for Students.

http://www.lib.uoguelph.ca/sites/default/files/fair_dealing_policy_0.pdf

Grades

The assignment of grades at the University of Guelph is based on clearly defined standards which are published in the Graduate Calendar for the benefit of faculty and students**.** In courses, which comprise a part of the student's program, standings will be reported according to the following schedule of grades and will use the following definitions for each of the numerical grade range (letter grades):

Table 2: Grade Interpretation

Percentage Grade	Letter Grade	Description
90-100	A+	**Outstanding.** The student demonstrated a mastery of the course material at a level of performance exceeding that of most scholarship students and warranting consideration for a graduation award.
80-89	A- to A	**Very Good to Excellent.** The student demonstrated a very good understanding of the material at a level of performance warranting scholarship consideration.
70-79	B	**Acceptable to Good.** The student demonstrated an adequate to good understanding of the course material at a level of performance sufficient to complete the program of study.
65-69	C	**Minimally Acceptable.** The student demonstrated an understanding of the material sufficient to pass the course but at a level of performance lower than expected from continuing graduate students.
0-64	F	An inadequate performance.

Further information on the Grades Schedule and Grade Interpretation can be found in the Graduate Calendar.

https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-as-gradesch.shtml

https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-as-gradeint.shtml

Graduate Student Responsibilities

From the choice of Advisor, choice of research project and through to degree completion, graduate students must recognize that they carry the primary responsibility for their success. The responsibilities assigned to Advisors, Advisory Committees and Departments provide the framework within which students can achieve success. Students should take full advantage of the knowledge and advice that the Advisor and Advisory Committee have to offer and make the effort to keep the lines of communication open. The Graduate Student Responsibilities are located in the Graduate Calendar.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

General Regulations

Graduates students are expected to be familiar with the General Regulations in the Graduate Calendar, including those related to university-wide policies on admission, registration, graduation, theses, fees and other subjects of importance to graduate students.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Plagiarism Detection Software

Students should be aware that faculty have the right to use software to aid in the detection of plagiarism or copying and to examine students orally on submitted work. For students found guilty of academic misconduct, serious penalties, up to and including suspension or expulsion from the University can be imposed.

Recording of Materials

Presentations which are made in relation to course work—including lectures—cannot be recorded or copied without the permission of the presenter, whether the instructor, a classmate or guest lecturer. Material recorded with permission is restricted to use for that course unless further permission is granted.

Storage and Retention of Videoconference Recordings[s23]

Courses may use videoconferencing-based software (e.g., Microsoft Teams, Zoom) and sessions may be recorded by your instructor. As a result, the University of Guelph may collect your image, voice, name, personal views and opinions, and course work under

the legal authority of the *University of Guelph Act* and in accordance with the *Freedom of Information and Protection of Privacy Act*. The recording may capture material shared on screen, participant audio and participant video and may be used to facilitate asynchronous learning by other students registered in the course. Recordings of this nature will be deleted following the conclusion of the course. Recordings that facilitate assessment will be retained for a period of one year following the conclusion of the course. If you have any questions about the collection and use of this information, please contact your instructor.

Disclaimer

Please note that the ongoing COVID-19 pandemic may necessitate a revision of the format of course offerings, changes in classroom protocols, and academic schedules. Any such changes will be announced via CourseLink and/or class email.

This includes on-campus scheduling during the semester, mid-terms and final examination schedules. All University-wide decisions will be posted on the COVID-19 website and circulated by email.

https://news.uoguelph.ca/2019-novel-coronavirus-information/

Illness

Medical notes will not normally be required for singular instances of academic consideration, although students may be required to provide supporting documentation for multiple missed assessments or when involving a large part of a course (e.g., final exam or major assignment).

Covid-19 Safety Protocols

For information on current safety protocols, follow these links:

How U of G Is Preparing for Your Safe Return

Guidelines to Safely Navigate U of G Spaces

Please note, these guidelines may be updated as required in response to evolving University, Public Health or government directives.

https://news.uoguelph.ca/return-to-campuses/how-u-of-g-is-preparing-for-your-safe-return/

https://news.uoguelph.ca/return-to-campuses/spaces/#ClassroomSpaces

BUS*6180 Financial and Managerial Accounting

Credit Weight: 0.50

Course Details

Calendar Description

This course emphasizes the gathering and use of financial information to facilitate effective financial and management decisions by managers to contribute towards overall corporate vision and exercise fiscal responsibility towards overall corporate results and governance. This course takes an accounting information user rather than supplier perspective.

Pre-Requisite(s): None

Co-Requisite(s): None

Restriction(s): Lang Executive Programs students only

Method of Delivery: Online

Course Website Access Date:

Course Start Date:

Course End Date:

Final Exam

There is no final exam in this course.

Instructional Support

Instructor

Louise Hayes

Email: lhayes02@uoguelph.ca
Telephone: (519) 824-4120 Ext. 58450
Office: MacDonald Hall (MAC), Room 205

Originally from British Columbia, Louise Hayes currently teaches in the Department of Management as well as in the MBA Program at the University of Guelph. Prior teaching experience includes various accounting and audit courses at the University of Guelph and other post-secondary institutions in Ontario.

Louise has taught accounting and audit for over twenty years, following seven years in public accounting, where she focused on IT audit. Louise is a member of CPA Ontario and British Columbia and is currently serving on the CPA Canada Audit and Assurance Technology Committee. Louise's research interests focus on determinants of financial reporting quality and the reporting of internal control weaknesses. She uses textual analysis and machine learning in her research.

Program Contact

Catherine Statton (Director, Executive Programs)

Email: cstatton@uoguelph.ca
Telephone: (519) 824-4120 Ext. 56607
Office: MacDonald Hall, Room 304

Learning Resources

Required Textbooks

Title: Cornerstones of Financial Accounting
Edition / Year: Third Canadian Edition / 2021
Publisher: Nelson

Title: Cornerstones of Managerial Accounting
Edition / Year: Third Canadian Edition / 2018
Publisher: Nelson

Supplementary Materials

This course includes supplementary materials. These materials are meant to supplement the required readings and course content. You can explore the materials at your own pace. To access these materials, select **Content** on the navbar to locate **Supplementary Materials** in the table of contents panel.

Course Website

CourseLink (powered by D2L's Brightspace) is the course website and will act as your classroom. It is recommended that you log in to your course website every day to check for announcements, access course materials, and review the weekly schedule and assignment requirements.

https://courselink.uoguelph.ca/

Ares

For this course, you will be required to access course reserve materials through the University of Guelph McLaughlin Library. To access these items, select **Ares** on the navbar in CourseLink. Note that you will need your Central Login ID and password in order to access items on reserve.

For further instructions on accessing reserve resources, visit How to Get Course Reserve Materials.

If at any point during the course you have difficulty accessing reserve materials, please contact the e-Learning Operations and Reserve Services staff at:

Tel: 519-824-4120 ext. 53621
Email: libres2@uoguelph.ca
Location: McLaughlin Library, First Floor, University of Guelph

https://www.lib.uoguelph.ca/find/course-reserves-ares

Learning Outcomes

Course Learning Outcomes

Accounting is the financial language of business. Top managers have a sound understanding of the framework of accounting and are comfortable with its uses. You will be expected to understand the accounting cycle and analyze the effects of business transactions on basic financial statements. You will also understand the basics of managerial accounting through contribution margin format income statements and cost-volume-profit analysis. A fundamental concept of financial analysis is the ability to identify which information is relevant to the issue at hand.

The course covers the basic concepts and applications in Financial Accounting, Managerial Accounting and Corporate Finance. An understanding of business finance and accounting is essential for all managers. As part of the management team, all managers need to contribute towards overall corporate vision, mission and value proposition and exercise their fiscal responsibility towards overall corporate results and governance.

Non-financial managers, as key members of the management team, need to appreciate how an understanding of finance can greatly add value in their roles as organizational strategic partners and decision makers. They are accountable for the planning, execution, evaluation, and control of their area of influence towards corporate objectives – Profitability, Sustainability and Growth of an organization.

By the end of this course, you should be able to:

1. Explain the nature of the Financial and Management accounting framework, along with Corporate Finance, and summarize their complementary aspects in organizational decision-making; and
2. Input and analyze key financial information and their implication – in consultation with financial managers – and add value by integrating strategy, operations, and performance.

These outcomes are usually attained through an understanding of:

- Overall corporate strategy and its financial impact in all functional areas;
- Financial statements: Income Statement, Statement of Financial Position, Cash flow – their analysis and interpretations - to improve overall efficiency and effectiveness;
- Product/Service Costing: Behavior and cost estimating within organizational context;
- Cost-volume-profit analysis: Relevance to short-term decisions;
- Pricing strategies: Short and long term decision models based on Product/Service lifecycles;
- Budgeting, Planning and Controls for analysis and continuous improvement;
- Decision Making / Capital Expenditure Decisions / Time Value of Money;
- Decentralization and Performance Evaluations: Application of Balanced Scorecard towards Planning, Control and Corporate Governance; and

Concepts are illustrated and discussed through problems, mini-cases, and a business simulation.

Teaching and Learning Activities

Method of Learning

Because learning in a graduate program is largely student driven, the Instructor's role in this course is as facilitator of student learning rather than as lecturer or conveyor of information. The instructor will point you in the direction of information resources, "the fishing rod", rather than simply giving you the answer, "the fish". The onus for learning is with you, and classmates are expected to help each other learn. You are strongly encouraged to discuss material with your classmates in the **Discussions** area prior to contacting the instructor.

The diversity in backgrounds of the students in the class means some will have more knowledge of accounting than others. This course is designed with the objective of building a common basis of understanding of both financial and managerial accounting. It is not intended to provide an in-depth examination of complex accounting and finance issues. For those of you who find that you are familiar with the materials presented and are interested in exploring complex issues, the instructor will provide you with additional readings and/or assignments.

Because this is a distance education course, feedback to you will be in writing. The purpose of giving you feedback is to constructively help you improve in your work. Comments about specific work and/or comments on how your work is organized and presented are meant to assist you in becoming a more effective communicator of financial information. Good communication skills are essential to success in any management role.

For those who require additional clarification of materials, the instructor will meet online by appointment at an arranged time as in a virtual office visit. This approach is used to facilitate everyone's varying time schedules. Contact your instructor directly to arrange an online meeting.

Weekly "coffee shops" will be offered through Zoom Webinar and Conferencing Service to provide opportunities to discuss the topics in real time and in a casual setting. Such venues allow your cohort to share resources and extend the conversations to the larger group (beyond your discussion group). While your instructor will host these "coffee shops", discussion topics are to be suggested by students, not by the instructor, i.e., these real-time discussions are not intended to be lectures. There is no obligation to attend.

Coffee shop and virtual office visit discussions will not be recorded. Your instructor will post matters of importance arising that are of interest to all students in CourseLink.

Course Structure

To support learning, there is a structured package of course material, and you must demonstrate your proficiency with the material. The course material has been divided into seven units:

- Unit 01: Introduction to Financial Accounting
- Unit 02: Accrual Accounting and Financial Statements
- Unit 03: Statement of Cash Flow & Financial Statement Analysis
- Unit 04: Cost Behavior

- Unit 05: Cost-Volume-Profit Analysis
- Unit 06: Control and Budgeting
- Unit 07: Relevant Information and Decision Making

What to Expect for Each Unit

Readings, problem solving, and self-study assignments are typical learning activities provided for each unit to facilitate learning of the course material. Through these activities, students are exposed to the material that is relevant to completing the graded quizzes, individual assignments, group project, and the final examination.

You are expected to complete each unit using the following study sequence:

1. Review **Unit Introduction**, **Learning Outcomes**, and **Readings** assigned by the instructor, including textbook reading and electronic reading/viewing placed on **Ares.**
2. Read **Instructor Commentary** given in the unit on the course website.
3. View **Demonstration Problems**. These animated simulations selected from the Cornerstone Videos that accompany the textbook are linked in the unit on the course website. These videos explain key concepts in each unit and are selected by your instructor to help you learn the necessary skills and procedures you need for your assignments.
4. Complete **Practice Activities**. This section is a very important self-study part of the course and is essential for understanding the course material and successfully completing graded assignments. Solutions are provided. **The multiple-choice questions on examinations will be based on these practice activities**. Practice activities provide you with a variety of learning activities to apply your knowledge and skills including:
    a. Discussion Questions (DQ): Each discussion question is designed to discuss terms and concepts presented in the chapter.
    b. Cornerstone Exercises (CSE): Each exercise applies single or multiple learning objectives from the textbook chapter and corresponds to a demonstration problem video.
    c. Brief Exercises (BE): These activities illustrate and apply a single learning objective from the textbook chapter.
    d. Exercises (E): These additional activities illustrate and apply single and multiple learning objectives from the textbook chapter.
    e. Problems (P): These activities are designed to develop decision-making skills.
    f. Skills-Development Cases (S): These activities are designed to develop analytical and critical thinking skills.

Course Success

A critical factor for success in this course is to stay on track with the course schedule. The average expected time commitment will be 20 hours per week. You can expect to spend from 15 hours to 25 hours or more depending on your previous accounting knowledge.

The following factors will significantly influence your success in this course:

1. Log in to your course website every day to, access course materials, review weekly schedule and assignment requirements, participate in online discussions and other learning activities indicated in the schedule.
2. Check for instructor's announcement in the **Announcements** section of the Course Home page.
3. Complete your assignments on time before the due date.
4. Read the assigned material and complete activities within the unit.
5. Work effectively and efficiently with your assigned group members.
6. Engage the instructor early if you have any issues.

Schedule

It is strongly recommended that you follow the course schedule provided below. The schedule outlines what you should be working on each week of the course and lists the important due dates for the assessments. By following the schedule, you will be better prepared to complete the assessments and succeed in this course.

Unit 01: Introduction to Financial Accounting

Week 1 –

Readings

- Website: Unit 01 Content
- Textbook – Cornerstones of Financial Accounting:
    - Ch. 1: Financial statements and decision making.
    - Ch. 2: The accounting information system and financial statements (pp. 62-80).
- Ares:
    - PBS.org. (2014). *True cost accounting: The Lexicon of Sustainability*. [Video].

Activities

- Familiarize yourself with the course website by selecting **Start Here** on the navbar.

- Review **Outline** and **Assessments** on the course website to learn about course expectations, assessments, and due dates.
- Confirm your access to the course reserve materials by selecting **Ares** on the navbar.
- Complete the **Practice Test** using Respondus through the **Quizzes** tool. It is important to complete this test during the first week of the course.
- Participate in the **Introductions Discussion** activity.

Assessments

- **Graded Quiz 1**
  Opens:
  Closes:

Unit 02: Accrual Accounting and Financial Statements

Week 2 –

Readings

- Website: Unit 02 Content
- Textbook – Cornerstones of Financial Accounting:
  - Ch. 3: Accrual accounting and financial statements (pp. 128-146; Note: bookkeeping details presented in Cornerstone 3.3, Cornerstone 3.4, Cornerstone 3.5, and Cornerstone 3.6 in these pages may be ignored).
  - Ch. 6: Reporting and analyzing inventory and cost of goods sold (pp. 308-315 and pp. 336-340).
- Ares:
  - Milstead, D. (2016). How companies play with the books. *The Globe and Mail*.

Assessments

- **Graded Quiz 2**
  Opens:
  Closes:
- **Individual Assignment 1**
  Due:

Unit 03: Statement of Cash Flow and Financial Statement Analysis

Week 3 –

Readings

- Website: Unit 03 Content
- Textbook – Cornerstones of Financial Accounting:
    - Ch. 11: Reporting and analyzing the statement of cash flows (pp. 626-648 and pp. 657-660).
    - Ch. 13: Analysis and interpretation of financial statements.

Assessments

- **Graded Quiz 3**
  Opens:
  Closes:

Unit 04: Introduction to Managerial Accounting

Week 4 –

Readings

- Website: Unit 04 Content
- Textbook – Cornerstones of Managerial Accounting:
    - Ch. 1: Introduction to managerial accounting.
    - Ch. 2: Basic managerial accounting concepts.

Assessments

- **Graded Quiz 4**
  Opens:
  Closes:

  Term Test 1 (covers content from Units 01-03)
  Opens:

- **Individual Assignment 2**
  Due:

Unit 05: Cost-Volume-Profit Analysis

Week 5 –

Readings

- Website: Unit 05 Content
- Textbook – Cornerstones of Managerial Accounting:
    - Ch. 3: Cost behaviour.
    - Ch. 4: Cost-volume-profit analysis: A managerial planning tool.

- Ares:
    - Bricklin, D. (2016). *Meet the inventor of the electronic spreadsheet.* TED Talks. [Video].

Assessments

- **Graded Quiz 5**
  Opens:
  Closes:
- **Group Project: Team Charter**
  Due:

Unit 06: Control and Budgeting

Week 6 –

Readings

- Website: Unit 06 Content
- Textbook – Cornerstones of Managerial Accounting:
    - Ch. 9: Budgeting, production, cash, and master budget.
    - Ch. 12: Performance evaluation and decentralization.
- Ares:
    - Churchill, N. C. (1984). Budget choice: Planning versus control. *Harvard Business Review*.

Assessments

- **Graded Quiz 6**
  Opens:
  Closes:

  Term Test 2 (covers content from Units 04-05)
  Opens:

  .

Unit 07: Relevant Information and Decision Making

Week 7 –

Readings

- Website: Unit 07 Content
- Textbook – Cornerstones of Managerial Accounting:

- Ch. 13: Short-run decision making: Relevant costing (pp. 628-644)
- Ch. 14: Capital investment decisions.

- Ares:
  - Nande, G. (2014) *The time value of money*. TED-Ed. [Video].
  - *Blockchain in Supply Chain* (2019). Blockchain Zoo. YouTube [Video]

Activities

- Assign a facilitator for the **Unit 08 Discussion with Video Summary.**

Assessments

- **Graded Quiz 7**
  Opens:
  Closes:
- **Group Project (written and video parts)**
  Due:

Assessments

The grade determination for this course is indicated in the following table. A brief description of each assessment is provided below. Select **Content** on the navbar to locate **Assessments** in the table of contents panel to review further details of each assessment. Due dates can be found under the Schedule heading of this outline.

Table 1: Course Assessments

Assessment Item	**Weight**
Online Quizzes (7 @ 5% each)	35%
Individual Assignment 1	10%
Individual Assignment 2	15%
Group Project • Team Charter • Written Assignment • Video Assignment	20%
Term Tests (2 @ 10%)	20%
Total	**100%**

Assessment Descriptions

Online Quizzes

The seven (7) online quizzes give you an opportunity to evaluate how well you have learned the unit material before you attempt the individual case assignments, group project, midterm exam, and final exam. Each quiz includes 15 multiple-choice questions selected at random from a test bank. You have one attempt at each quiz.

Individual Assignments

Case studies provide you with an opportunity to apply the knowledge gained from the course to hypothetical situations. In the process, you will be challenged to think critically and analytically. Throughout this course, you are asked to complete two (2) case study assignments. When responding to these assignments, you should be concise and to the point. After reading each fact situation, try to identify as many issues or concepts that might be relevant to the particular case(s). If you need to, go back to the readings to jog your memory regarding the relevant concepts.

Group Project

For this project, you will be working in the group of 3-4 students to apply the knowledge gained from the course. The group will use financial information to make a business decision.

Term Tests

The term tests will consist of both multiple choice and short answer questions.

The term tests will be delivered online via the **Quizzes** tool using Respondus LockDown Browser and Monitor.

This course requires the use of Respondus LockDown Browser and Monitor (webcam) to proctor your online Term Tests within CourseLink. Use of Lockdown Browser with a webcam has been implemented to maintain the academic integrity of the exams. You must download and install LockDown Browser and Monitor to complete the practice test and the two term tests. While writing the practice test and each term test, you must show your university issued identification card during the Respondus Startup Sequence.

Please be sure to review the Using Respondus Lockdown Browser and Monitor instructions by selecting **Content** on the navbar to locate **Assessments** in the table of contents panel.

Important Note: There is a mandatory practice test that you are required to take before the online term test. The purpose of the practice test is to ensure that Respondus LockDown Browser and Monitor is set up properly and that you are comfortable using the software.

If you have any questions regarding the use of Respondus Lockdown Browser and Monitor or if you encounter any technical issues during the practice test or final exam,

please contact CourseLink Support at courselink@uoguelph.ca or 519-824-4120 ext. 56939.

http://www.respondus.com/lockdown/download.php?id=273932365

Course Technology Requirements and Technical Support

CourseLink System Requirements

You are responsible for ensuring that your computer system meets the necessary system requirements. Use the browser check tool to ensure your browser settings are compatible and up to date. (Results will be displayed in a new browser window).

https://opened.uoguelph.ca/student-resources/system-and-software-requirements

https://courselink.uoguelph.ca/d2l/systemCheck

Microsoft Excel Requirements

This course uses Microsoft Excel, a spreadsheet tool. To learn more about installing Microsoft Office through the Office 365 Portal, please visit the University's Computing & Communications Services website.

https://www.uoguelph.ca/ccs/software/supported-products/office365

Respondus LockDown Browser and Monitor Requirements

Respondus LockDown Browser is a locked browser for taking quizzes in CourseLink. It prevents you from printing and copying; using other operating software; using search engines (e.g., going to another URL); communicating via instant messaging; and it blocks non-web-related software (e.g., Adobe PDF, Microsoft Word).

Respondus Monitor is a companion application for LockDown Browser that uses webcam and video technology to ensure academic integrity during online exams. The software captures video during the exam and allows the instructor to review the video once the exam is completed.

In order to use Respondus LockDown Browser and Monitor, you must meet the following technical requirements so that you can take the practice test and final exam:

1. Operating Systems: Windows 10, 8, 7; Mac OS X 10.10 or higher.
2. Memory: Windows 2 GB RAM; Mac 512 MB RAM.
3. For Mac users: Safari must function properly on the computer.
4. Functioning webcam and microphone. The webcam and microphone can be built into your computer or can be the type that plugs in with a USB cable. (You will be required to do an environment scan of your room, so please ensure you can move your computer, laptop, or webcam for this scan.)

5. A broadband Internet connection. It is recommended that you access the Internet via a wired connection.

If you have any concerns about meeting the necessary system requirements, contact CourseLink Support. They will work with you to find alternative solutions or make alternative arrangements.

https://opened.uoguelph.ca/student-resources/system-and-software-requirements

https://support.opened.uoguelph.ca/contact

Microsoft Teams System Requirements

This course may use **Microsoft Teams** as a video communication tool. A Webcam, a microphone to record video, and headphones/speakers to play back the recording are also needed. In order to use **Microsoft Teams**, you must meet the following technical requirements:

1. An internet connection – broadband wired or wireless (3G or 4G/LTE);
2. Speakers and a microphone – built-in or USB plug-in or wireless Bluetooth;
3. A webcam or HD webcam - built-in or USB plug-in;
4. Supported mobile platforms: Android 4.4 or later and iOS 10.0 or later.

Technical Skills

As part of your online experience, you are expected to use a variety of technology as part of your learning:

- Manage files and folders on your computer (e.g., save, name, copy, backup, rename, delete, and check properties);
- Install software, security, and virus protection;
- Use office applications (e.g., Word, PowerPoint, Excel, or similar) to create documents;
- Be comfortable uploading and downloading saved files;
- Communicate using email (e.g., create, receive, reply, print, send, download, and open attachments);
- Navigate the CourseLink learning environment and use the essential tools, such as **Dropbox**, **Quizzes**, **Discussions**, and **Grades** (the instructions for this are given in your course);
- Access, navigate, and search the Internet using a web browser (e.g., Firefox, Chrome. **NOTE**: Internet Explorer should not be used for the Business Simulation); and
- Perform online research using various search engines (e.g., Google) and library databases.

Technical Support

If you need any assistance with the software tools or the CourseLink website, contact CourseLink Support.

CourseLink Support
University of Guelph
Day Hall, Room 211
Email: courselink@uoguelph.ca
Tel: 519-824-4120 ext. 56939
Toll-Free (CAN/USA): 1-866-275-1478

Walk-In Hours (Eastern Time):
Monday thru Friday: 8:30 am–4:30 pm

Phone/Email Hours (Eastern Time):
Monday thru Friday: 8:30 am–8:30 pm
Saturday: 10:00 am–4:00 pm
Sunday: 12:00 pm–6:00 pm

Course Specific Standard Statements

Acceptable Use

The University of Guelph has an Acceptable Use Policy, which you are expected to adhere to.

https://www.uoguelph.ca/ccs/infosec/aup

Communicating with Your Instructor

During the course, your instructor will interact with you on various course matters on the course website using the following ways of communication:

- **Announcements:** The instructor will use **Announcements** on the Course Home page to provide you with course reminders and updates. Please check this section frequently for course updates from your instructor.
- **Ask Your Instructor Discussion:** Use this discussion forum to ask questions of your instructor about content or course-related issues with which you are unfamiliar. If you encounter difficulties, the instructor is here to help you. Please post general course-related questions to the discussion forum so that all students have an opportunity to review the response. To access this discussion forum, select **Discussions** from the **Tools** dropdown menu.
- **Email:** If you have a conflict that prevents you from completing course requirements, or have a question concerning a personal matter, you can send your instructor a private message by email. The instructor will respond to your email within 48 to 72 hours.

- **Online Meetings:** If you have a complex question you would like to discuss with your instructor, you may book an online meeting. Online meetings depend on the availability of you and the instructor, and are booked on a first come first served basis.

Netiquette Expectations

For distance education courses, the course website is considered the classroom and the same protections, expectations, guidelines, and regulations used in face-to-face settings apply, plus other policies and considerations that come into play specifically because these courses are online.

Inappropriate online behaviour will not be tolerated. Examples of inappropriate online behaviour include:

- Posting inflammatory messages about your instructor or fellow students;
- Using obscene or offensive language online;
- Copying or presenting someone else's work as your own;
- Adapting information from the Internet without using proper citations or references;
- Buying or selling term papers or assignments;
- Posting or selling course materials to course notes websites;
- Having someone else complete your quiz or completing a quiz for/with another student;
- Stating false claims about lost quiz answers or other assignment submissions;
- Threatening or harassing a student or instructor online;
- Discriminating against fellow students, instructors, and/or TAs;
- Using the course website to promote profit-driven products or services;
- Attempting to compromise the security or functionality of the learning management system;
- Sharing your username and password; and
- Recording lectures without the permission of the instructor.

Submission of Assignments to Dropbox

The Group Project Team Charter, Individual Assignments 1 and 2, as well as the Group Project (both written and video parts) should be submitted electronically via the online **Dropbox** tool.

When submitting your assignments using the **Dropbox** tool, do not leave the page until your assignment has successfully uploaded. To verify that your submission was complete, you can view the submission history immediately after the upload to see

which files uploaded successfully. The system will also email you a receipt. Save this email receipt as proof of submission.

Be sure to keep a back-up copy of all of your assignments in the event that they are lost in transition. In order to avoid any last-minute computer problems, your instructor strongly recommend you save your assignments to a cloud-based file storage (e.g., Google Docs), or send to your email account, so that should something happen to your computer, the assignment could still be submitted on time or re-submitted.

It is your responsibility to submit your assignments on time as specified on the Schedule. Be sure to check the technical requirements and make sure you have the proper computer, that you have a supported browser, and that you have reliable Internet access. Remember that **technical difficulty is not an excuse not to turn in your assignment on time.** Don't wait until the last minute as you may get behind in your work.

If, for some reason, you have a technical difficulty when submitting your assignment electronically, please contact your instructor or CourseLink Support.

https://support.opened.uoguelph.ca/contact

Late Policy

If you choose to submit your individual assignments to the **Dropbox** tool late, the full allocated mark will be reduced by 10% per day after the deadline for the submission of the assignment.

For late term test submissions to the **Quizzes** tool, your attempt will be flagged as late, and you will be prevented from making further changes to your attempt once your time ends. Make sure you save all your responses to the test questions.

For details on how long you have to complete the tests, please see the instructions in **Assessments** on CourseLink. The **Quizzes** tool counts down your time in the upper-left hand corner. Please pay close attention to this countdown and save your answers frequently.

Extensions will be considered for medical reasons or other extenuating circumstances. If you require an extension, discuss this with the instructor as soon as possible and well before the due date. Barring exceptional circumstances, extensions will not be granted once the due date has passed. These rules are not designed to be arbitrary, nor are they inflexible. They are designed to keep you organized, to ensure that all students have the same amount of time to work on assignments, and to help to return marked materials to you in the shortest possible time.

Obtaining Grades and Feedback

Unofficial assessment marks will be available in the **Grades** tool of the course website.

Your instructor will have grades posted online within 7-10 days of the submission deadline if the assignment was submitted on time. Once your assignments are marked you can view your grades on the course website by selecting **Grades** from the **Tools**

dropdown menu on the navbar. Your course will remain open to you for one year following the end of your program.

Final grades will be available at the end of the semester. Students can access their final grade by logging into WebAdvisor (using your U of G central ID).

https://webadvisor.uoguelph.ca

Rights and Responsibilities When Learning Online

The course website is considered the classroom and the same protections, expectations, guidelines, and regulations used in face-to-face settings apply, plus other policies and considerations that come into play specifically because these courses are online.

For more information on your rights and responsibilities when learning in the online environment, visit Rights and Responsibilities.

http://opened.uoguelph.ca/student-resources/rights-and-responsibilities

Turnitin Originality Check

In this course, your instructor will be using Turnitin, integrated with the CourseLink **Dropbox** tool, to detect possible plagiarism, unauthorized collaboration or copying as part of the ongoing efforts to maintain academic integrity at the University of Guelph.

All individual assignments submitted to the **Dropbox** tool will be included as source documents in the Turnitin.com reference database solely for the purpose of detecting plagiarism of such papers. Use of the Turnitin.com service is subject to the Usage Policy posted on the Turnitin.com site.

A major benefit of using Turnitin is that you will be able to educate and empower yourself in preventing academic misconduct. In this course, you may screen your own assignments through Turnitin as many times as you wish before the due date. You will be able to see and print reports that show you exactly where you have properly and improperly referenced the outside sources and materials in your assignment.

Program Specific Standard Statements

Equity, Diversity, and Inclusion

At the Lang School of Business and Economics, we are committed to developing leaders with a social conscience, an environmental sensibility, and a commitment to their communities. A core tenet within this vision is that diversity is a strength with which we can experience greater connection and understanding.

As such, we affirm the importance and shared responsibility of our students, faculty, and staff creating and promoting equity and inclusion within our learning spaces. Creating these kinds of learning cultures is a process, not a destination; it requires ongoing willingness on the part of each person to thoughtfully and critically listen, unlearn, learn,

and engage as they are exposed to a multitude of perspectives and lived experiences. We encourage dialogues between students and instructors to address and advance opportunities for fostering greater diversity and inclusion in the learning environment. Openness to conversations with each other enables us to reflect and grow as we learn from one another respectfully and holistically.

As a department that is training the professionals of the future, we expect our learning spaces to abide by all institutional policies and guidelines, in particular those outlined by the Office of Diversity and Human Rights and the University of Guelph Human Rights Policy. Discrimination and harassment, as defined by our policies, will not be tolerated. Individuals should inform the appropriate party as per University policies if they experience any such behaviours.

https://www.uoguelph.ca/diversity-human-rights/human-rights-policy-and-procedures

---

University Standard Statements

University of Guelph: Graduate Policies

As a student of the University of Guelph, it is important for you to understand your rights and responsibilities and the academic rules and regulations that you must abide by. Consult the Graduate Calendar for the rules, regulations, curricula, programs and fees for current and previous academic years.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Email Communication

As per university regulations, all students are required to check their uoguelph.ca e-mail account regularly: e-mail is the official route of communication between the University and its students.

When You Cannot Meet Course Requirements

When you find yourself unable to meet an in-course requirement due to illness or compassionate reasons, please advise your course instructor (or designated person such as a teaching assistant) **in writing**, with your name, ID number and email contact.

Review the Graduate Calendar for information on regulations and procedures for Academic Consideration.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Drop Date

The last date to drop one-semester courses, without academic penalty, is indicated in the Schedule of Dates section of the Graduate Calendar. Review the Graduate Calendar for regulations and procedures for Dropping Courses.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Copies of Out-of-Class Assignments

Keep paper and/or other reliable back-up copies of all assignments: you may be asked to resubmit work at any time.

Accessibility

The University of Guelph is committed to creating a barrier-free environment. Providing services for students is a shared responsibility among students, faculty, and administrators. This relationship is based on respect of individual rights, the dignity of the individual and the University community's shared commitment to an open and supportive learning environment.

Students requiring service or accommodation, whether due to an identified, ongoing disability or a short-term disability should contact Accessibility Services as soon as possible.

For more information, contact Accessibility Services at 519-824-4120 ext. 56208, email Accessibility Services or visit the Accessibility Services website.

accessibility@uoguelph.ca

https://wellness.uoguelph.ca/accessibility/

Academic Misconduct

The University of Guelph is committed to upholding the highest standards of academic integrity and it is the responsibility of all members of the University community – faculty, staff, and students – to be aware of what constitutes academic misconduct and to do as much as possible to prevent academic offences from occurring. University of Guelph students have the responsibility of abiding by the University's policy on academic misconduct regardless of their location of study; faculty, staff and students have the responsibility of supporting an environment that discourages misconduct. Students need to remain aware that instructors have access to and the right to use electronic and other means of detection.

The Academic Misconduct Policy is detailed in the Graduate Calendar.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Copyright

Content within this course is copyright protected. Third party copyrighted materials (such as book chapters and articles) have either been licensed for use in this course, or have been copied under an exception or limitation in Canadian Copyright law.

The fair dealing exemption in Canada's Copyright Act permits students to reproduce short excerpts from copyright-protected materials for purposes such as research, education, private study, criticism, and review, with proper attribution. Any other

copying, communicating, or distribution of any content provided in this course, except as permitted by law, may be an infringement of copyright if done without proper license or the consent of the copyright owner. Examples of infringing uses of copyrighted works would include uploading materials to a commercial third party web site, or making paper or electronic reproductions of all, or a substantial part, of works such as textbooks for commercial purposes.

Students who upload to CourseLink copyrighted materials such as book chapters, journal articles, or materials taken from the Internet, must ensure that they comply with Canadian Copyright law or with the terms of the University's electronic resource licenses.

For more information about students' rights and obligations with respect to copyrighted works, review Fair Dealing Guidance for Students.

http://www.lib.uoguelph.ca/sites/default/files/fair_dealing_policy_0.pdf

Grades

The assignment of grades at the University of Guelph is based on clearly defined standards which are published in the Graduate Calendar for the benefit of faculty and students**.** In courses, which comprise a part of the student's program, standings will be reported according to the following schedule of grades and will use the following definitions for each of the numerical grade range (letter grades):

Table 2: Grade Interpretation

Percentage Grade	Letter Grade	Description
90-100	A+	**Outstanding.** The student demonstrated a mastery of the course material at a level of performance exceeding that of most scholarship students and warranting consideration for a graduation award.
80-89	A- to A	**Very Good to Excellent.** The student demonstrated a very good understanding of the material at a level of performance warranting scholarship consideration.
70-79	B	**Acceptable to Good.** The student demonstrated an adequate to good understanding of the course material at a level of performance sufficient to complete the program of study.

Percentage Grade	Letter Grade	Description
65-69	C	**Minimally Acceptable.** The student demonstrated an understanding of the material sufficient to pass the course but at a level of performance lower than expected from continuing graduate students.
0-64	F	An inadequate performance.

Further information on the Grades Schedule and Grade Interpretation can be found in the Graduate Calendar.

https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-as-gradesch.shtml

https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-as-gradeint.shtml

Graduate Student Responsibilities

From the choice of Advisor, choice of research project and through to degree completion, graduate students must recognize that they carry the primary responsibility for their success. The responsibilities assigned to Advisors, Advisory Committees and Departments provide the framework within which students can achieve success. Students should take full advantage of the knowledge and advice that the Advisor and Advisory Committee have to offer and make the effort to keep the lines of communication open. The Graduate Student Responsibilities are located in the Graduate Calendar.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

General Regulations

Graduates students are expected to be familiar with the General Regulations in the Graduate Calendar, including those related to university-wide policies on admission, registration, graduation, theses, fees and other subjects of importance to graduate students.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Plagiarism Detection Software

Students should be aware that faculty have the right to use software to aid in the detection of plagiarism or copying and to examine students orally on submitted work. For students found guilty of academic misconduct, serious penalties, up to and including suspension or expulsion from the University can be imposed.

Recording of Materials

Presentations which are made in relation to course work—including lectures—cannot be recorded or copied without the permission of the presenter, whether the instructor, a classmate or guest lecturer. Material recorded with permission is restricted to use for that course unless further permission is granted.

Storage and Retention of Videoconference Recordings

Courses may use videoconferencing-based software (e.g., Microsoft Teams, Zoom) and sessions may be recorded by your instructor. As a result, the University of Guelph may collect your image, voice, name, personal views and opinions, and course work under the legal authority of the *University of Guelph Act* and in accordance with the *Freedom of Information and Protection of Privacy Act*. The recording may capture material shared on screen, participant audio and participant video and may be used to facilitate asynchronous learning by other students registered in the course. Recordings of this nature will be deleted following the conclusion of the course. Recordings that facilitate assessment will be retained for a period of one year following the conclusion of the course. If you have any questions about the collection and use of this information, please contact your instructor.

COVID-19 Disclaimer

Please note that the ongoing COVID-19 pandemic may necessitate a revision of the format of course offerings and academic schedules. Any such changes will be announced via CourseLink and/or class email. All University-wide decisions will be posted on the University's COVID-19 website and circulated by email.

The University will not require verification of illness (doctor's notes). However, requests for Academic Consideration may still require medical documentation as appropriate

LEAD*6200 Leadership of Organizational Change

Winter 2022

Credit Weight: 0.50

Course Details

Calendar Description

This course studies the role of leadership in the management of change within an organization and the changes required of management. The course examines the development of trust, the building of organizational loyalty, and motivation and inspiring of high performance teams.

Pre-Requisite(s): None

Co-Requisite(s): None

Restriction(s): Lang Executive Programs students only

Method of Delivery: Online

Course Website Access Date:

Course Start Date:

Course End Date:

Final Exam

There is no final exam in this course.

Instructional Support

Instructor

Jamie Gruman

Email: jgruman@uoguelph.ca
Telephone: (519) 824-4120 Ext. 58730
Office: MacDonald Hall (MAC), Room 226

I'm Dr. Jamie Gruman, and I'll be your guide as we navigate the world of leadership and organizational change. You'd probably like to know a little bit about me. Well, here's the bio that I send to people when I give talks at conferences or companies:

Jamie Gruman earned his Ph.D. in the Applied Social Psychology Program at the University of Windsor in Ontario, Canada, where he specialized in organizational psychology. He has taught in the Psychology Department and the Department of Management at the University of Toronto, in the Psychology Department and the Odette School of Business at the University of Windsor and is currently an Associate Professor of Organizational Behaviour in the Department of Management at the University of Guelph. He has also served as an adjunct professor in the Faculty of Applied Health Sciences at the University of Waterloo and is the founding Chair of the Canadian Positive Psychology Association. He has been nominated for numerous teaching awards including two nominations as Ontario's best lecturer, and in 2009 was the recipient of a University of Guelph Distinguished Professor Award. An award-winning researcher, he has published articles in such journals as *Basic and Applied Social Psychology*, *The Journal of Vocational Behavior*, *Industrial and Organizational Psychology*, *Human Resource Management Review*, *Human Resource Development Quarterly, The Journal of Managerial Psychology, and Human Resource Management*, which is on the Financial Times list of the world's top management journals. His market-leading textbook on Applied Social Psychology, is now in a 3rd edition and is sold world-wide.

Dr. Gruman's research and writing have been reported by media outlets around the globe. In Canada he has been featured and quoted across the country in print and online in magazines such as MoneySense, Canadian Business, and Chatelaine, trade journals such as HR Professional and Public Sector Digest, and newspapers in every major Canadian city. He has appeared on CTV's Canada AM, Global News, Report on Business Television, CBC's The National, and has been syndicated on CBC radio. In addition to speaking at numerous academic and professional conferences, including those of the Academy of Management, the Conference Board of Canada, and TEDx, Dr. Gruman has consulted and delivered seminars for Fortune 500 corporations, public, and not-for-profit organizations including General Motors, Departments and Agencies of the Government of Canada, and the Children's Wish Foundation.

For more information on your instructor, please see the Welcome section under **Content** on the CourseLink website.

Office Hours Office hours will be held via the same **Zoom** link used to hold class. Appointments are necessary. Please email the instructor to set up an appointment. Please note that further details will be posted in the **Announcements**. See also **Communicating with Your Instructor.**

Program Contact

Catherine Statton (Director, Executive Programs)

Email: cstatton@uoguelph.ca
Telephone: (519) 824-4120 Ext. 56607
Office: MacDonald Hall, Room 304

Learning Resources

Required Textbooks

Title: Leading Quietly: An Unorthodox Guide to Doing the Right Thing
Author(s): Badarracco, J. L.
Edition / Year: 1st edition, 2002
Publisher: Harvard Business School Press
ISBN: 978-1578514878

The textbook is provided and will be shipped to registered students in advance of the course start date.

Course Website

CourseLink (powered by D2L's Brightspace) is the course website and will act as your classroom. It is recommended that you log in to your course website every day to check for announcements, access course materials, and review the weekly schedule and assignment requirements.

https://courselink.uoguelph.ca/

Ares

For further instructions on accessing reserve resources, visit How to Get Course Reserve Materials.

If at any point during the course you have difficulty accessing reserve materials, please contact the e-Learning Operations and Reserve Services staff at:

Tel: 519-824-4120 ext. 53621
Email: libres2@uoguelph.ca
Location: McLaughlin Library, First Floor, University of Guelph

https://www.lib.uoguelph.ca/find/course-reserves-ares

Learning Outcomes

Course Learning Outcomes

Welcome to LEAD*6200. This course is designed to address key topics in change management and some of the leadership issues associated with implementing important changes in organizations. In designing this course, I have tried to create a course on change management that I would want to take myself. If I took such a course, I would want it to be academically rigorous, comprehensive, intellectually stimulating, cover key topics in the subject area, and, of course, practically relevant. At the end of a graduate course on change management I would want to feel smart, as though I've been armed with high-quality knowledge about change, and prepared to at least begin to tackle real-world changes head on (and make mistakes from which I will learn a lot). FYI, this course took almost a year to develop initially, has been tweaked over the years, and underwent a major facelift in 2017 when about half of the readings were revised. I hope it meets your expectations and that you feel it is as good as any organizational change course you could have taken at Harvard, Stanford, or any other top-tier university. Guelph is a great school and I hope you consider this a great course. Please do not hesitate to provide me with feedback on how you think it can be improved, anytime. I welcome your input. In fact, I need your input if I am to understand how this course is perceived by my students and where they think changes to the course may be warranted. Don't be shy.

This course is focused on exposing you to important content, and having you engage in thought, discussions and assignments to drive home key lessons. The primary focus is not on self-understanding, or self-reflection. As we will see, self-knowledge can and does play a role in effecting change, however you will get enough of that in other courses. We will focus primarily on content.

At this point in the program, you have probably noted that each course you take has a different **personality**. This occurs as a result of the course structure, assignments, general instructions, and actual personality of the instructor (this occurs in off-line, face-to-face courses as well as these online ones). In the interest of promoting your comfort with the shift from one course to the next, I just wanted to highlight that you should expect the **personality** of this course to be different from those you have taken previously, and those you will take subsequently. For example, in some of your courses you complete numerous assignments and receive copious amount of feedback. In this course you will complete only a few, strategically chosen assignments and after each one you will receive a standardized feedback sheet containing only as much written feedback as necessary to highlight the major issues associated with the project objectives, and to orient you towards even greater success in future work (typically one or two short paragraphs).

I've structured this course in a manner similar to the kind of courses I took as a graduate student. Each week you will read a number of discrete articles and/or chapters that are connected only in terms of their general themes. Synthesizing the readings into

a coherent mental model is left to you (with help from your fellow students, and me, with whom you can discuss connections and distinctions). Some people find this challenging. That's good. It's part of growing as a leader. CEOs, Executive Directors, and other leaders are not provided with pre-packaged, coherent sets of information that tell them how to lead their organizations (even reports commissioned from consultants require critical analysis and integration). Instead, leaders need to create sense out of chaos by selectively attending to, interpreting, and synthesizing information. This sense-making approach is paralleled in this course in order to teach you something about the process of leading in addition to some of the content.

Organizational change is a complicated topic, and the competencies required to manage change successfully require years of experience to develop fully. You cannot master the leadership of change in seven-week course. However, you can certainly begin the process of building the knowledge and skills required to understand, promote, and sustain changes in organizations.

By the end of this course, you should be able to:

1. Demonstrate an understanding of some of the key issues in organizational change and be able discuss the topic intelligently with others who know about the topic;
2. Distinguish between valid knowledge about change and trivial pablum;
3. Analyze an organization for the purpose of developing a strategy to lead a change effort;
4. Design a process for promoting change in an organization;
5. Implement some skills related to change management (i.e., communication);
6. Explain different approaches to organizational change and some of the contingencies that can affect its success;
7. Identify potential weak points that could undermine a change effort, and address sources of resistance to change;
8. Critically analyze new information regarding change that you may encounter; and
9. Explain some of the finer points of how to act as the leader of changes in an organization.

Teaching and Learning Activities

Method of Learning

Our online discussions and assignments will undoubtedly contribute to your knowledge about leadership and change management. Remember, however, that the readings included in our course have all been carefully chosen from among the hundreds of thousands of articles and books on these topics that are in print (some people suggest

that over a million pieces have been written on organizational change). Bear this in mind as you read the assigned materials. Much of the development of this course involved spending many months discriminating among these materials and judiciously choosing the ones for you to read. Each reading represents what I believe to be a key issue in leadership and change. You should approach each article and chapter as a unique lesson unto itself and try to discern the crucial issue(s) within each one. Then, present your assessment to the group along with any addition, criticism, elaboration, or integration you think is warranted.

Although you may choose to respond, or not, to specific postings of your course-mates, please assume that when I, myself, pose a question, I am expecting everyone to post a response, or at least to think carefully about a response that could be provided. As noted below, asking questions is one of the key ways I will direct your thinking about leadership and change, so please treat my questions as part of the course structure. Remember that the questions I pose are meant to help direct your learning and that you will get the most out of this course by actively engaging with these questions.

Course Structure

The course is organized into the following seven units:

- Unit 01: Introduction to Change Management
- Unit 02: The Planned Approach to Change
- Unit 03: The Emergent Approach to Change
- Unit 04: Sources of and Approaches to Dealing with Resistance
- Unit 05: Points of Leverage
- Unit 06: Integration/Contingency
- Unit 07: Changing Quietly

What to Expect for Each Unit

At the beginning of each unit, I will post a brief overview of our week's readings and learning goals to help orient you to the material. At the end of each unit, I will summarize some of the week's ideas and discuss where we've been in terms of the material from previous weeks to help you keep your bearings as we make our way through the course. Please feel free to ask me questions if anything is ever unclear.

I will be online most, but not all, weekdays. I will try to respond to every e-mail /direct question in the General Discussion Area within one business day, and will always respond within two business days, barring unforeseen circumstances. I sometimes visit the site on weekends, so you may receive responses on Saturday or Sunday. Please understand if, on rare occasions, I take slightly longer to respond. None of our lives gets put on hold during this course, and seven weeks is a long time to expect no other urgent matters to arise. I will try to advise you if my responses may be delayed.

I will not be checking your Assignment Groups (case study groups) for messages. These groups are your opportunity to produce independent group work. However, if you have a question about assignments, by all means, e-mail me as soon as any questions arise.

In your General Discussion groups, I will submit my "two cents" as appropriate throughout the course. I may elaborate on ideas, post a question, redirect a conversation, or initiate a discussion. I may even post ideas with which I do not agree in order to stimulate discussion about this issue. As moderator of the course, I also need to ensure that we stay on track. One way I do this is by carefully choosing the postings to which I respond. It is very easy for us to get off track and/or to start delving into areas that, while really interesting, are not quite pertinent to the lesson objectives. If I do not elaborate on one of your postings, please do not feel snubbed (I will, of course, always respond to direct questions). I may also ask that people redirect a conversation to another discussion area.

Sometimes I will provide answers to questions, but oftentimes I will simply ask questions and let you grapple with the answers yourselves. In fact, I may even sometimes end units with questions. I will do this to encourage you to think about ideas and to try to provide you with a high-quality education. As Warren Bennis notes in his 1989 book *On Becoming a Leader,* education is very different from training. Training is firm, static, involves facts, dogma, passivity, and a focus on answers. Education, by contrast, is tentative, dynamic, involves ideas, discovery, active exploration, and a focus on questions. This course (and program) is about education, not training. Your (work) life is too complicated for me to be able to give you all the right answers to situations we may discuss, but I can definitely get you thinking about the right questions.

Additionally, you might be interested to know that a number of authors/management thinkers suggest that effective leadership involves asking the right questions, as opposed to having all the answers. I will try to model this behaviour while simultaneously providing you with knowledge to help guide you in your development as a leader. So, don't just sit back and wait for me to provide answers to questions that are posed in the Discussion forums. Often, I will purposefully choose not to post my two cents, or wait a while until I do, because I want you to generate the answer, or multiple answers, yourselves.

As indicated above, although I will, of course, participate in, and sometimes guide, our General Discussions, if the class is participating effectively, I should fade into the background. My objective is to act more as a facilitator (a guide on the side), than a director (a sage on the stage). Although direction is sometimes needed, I, myself, should not be the focus of our course. Distance education requires greater involvement on the part of students than traditional courses. Research shows that distance learners who are more proactive are more satisfied with their courses, and rate the quality of learning higher than those who are less proactive (see Kickul, G. & Kickul, J. (2006). Closing the gap: impact of proactivity and learning goal orientation on e-learning outcomes. *International Journal on E-learning,* 5(3), 361-372). So, again, don't wait for me to provide answers or responses to posted questions, debates, controversies, or ideas. I may do so, but so should you. Engage with the group. This is an experienced,

competent group of folks. You should try to capture and exploit the collective wisdom of all group members and evaluate each other's ideas by drawing on the weekly readings.

Ultimately, what you take away from this course is directly proportional to what you put into it. When you read the assigned material, think about it and try to apply it to your own experiences wherever you can. This will enhance the lessons and hasten your learning Also, use the group (and me) to test out your ideas. Post questions. Follow-up on others' ideas. Politely disagree with people and explain why. Say why you think one of the readings is bad (and be prepared to defend yourself with strong arguments). Say why you think one of the readings is great (and compliment the professor's awesome judgment in choosing it). Get out of your comfort zone. This is an opportunity to play with ideas that may affect your leadership ability for the rest of your career!

About the Readings

Some of the papers included in the course readings are old. Some students complain about this in the course evaluation and say they want to read more current works. That is a mistake. When you learn about any topic what you should want to read are the most important pieces on the topic, not necessarily the most current ones. Many of these most important pieces are considered “seminal”. They stand the test of time because they are full of timeless wisdom. Contemporary articles and books of high quality will cite these seminal works, thus demonstrating the authors’ thorough understanding of the subject. Let me give you an example. In a 2017 article called “Evolutionary Psychology: A How-To Guide” the authors - one of whom is David Buss, the world’s leading expert on the topic - cite multiple old articles including three dating all the way back to the 1960’s! In the world of work people tend to be attracted to new ideas the same way they’re attracted to new technologies. But leadership knowledge isn’t like cell phone technology. New is not necessarily better. In the world of academia, we certainly don’t ignore contemporary works, but we’re equally interested in the time-tested ideas that are contained in classic and seminal works. Wisdom has no expiry date.

Although dated, none of the articles in our course are outdated. I’ve included them because I believe they're still among the best readings for helping you to get your heads around the topics we're covering. The knowledge required for effective management and leadership doesn’t change very much over time. If you take a look at Henry Mintzberg’s 2009 book entitled “Managing” he cites relevant research dating all the way back to the 1950’s. Mintzberg, one of the greatest management thinkers of our time, notes that “Despite the great fuss we make about change, the fact is that the basic aspects of human behavior - and what could be more basic that managing and leading? – remain rather stable” (p. 14).

Any time you’re interested in other, possibly more contemporary, articles on each week’s topic, check out our weekly lists of additional readings.

Group Work

Professional programs are great because they brings together all sorts of motivated people from many different backgrounds and tons of varied experiences. Undoubtedly,

you will learn things not only from me and the readings, but from your fellow students. Every executive education instructor I know, from top institutions around the world, says that they learn as much from their students as the students learn from them. This course will be no different. I look forward to reading about your thoughts and experiences.

A Note about Sources

I draw on many literary sources in this course. One I rely on heavily is Bernard Burnes' *Managing Change* (4th ed.). I haven't included this book as part of the course readings because it is fairly heavy reading, and mammoth at about 600 pages. Requiring you to read Burnes' book would simply be too much work for you. So, I will be summarizing some of Burnes' work through comments I make in the course (when you think I sound smart, it's probably just me summarizing Burnes' ideas). For those of you who are particularly interested in the organizational theory that underlies change, I recommend this book.

Schedule

It is strongly recommended that you follow the course schedule provided below. The schedule outlines what you should be working on each week of the course and lists the important due dates for the assessments. By following the schedule, you will be better prepared to complete the assessments and succeed in this course.

Unit 01: Introduction to Change Management

Week 1 –

Readings

- CourseLink Website: Unit 01 Content
- Ares:
    - Kotter, J.P. (2001). What Leaders Really Do, The Best of Harvard Business Review, 79(11), 85–96. Copyright © 2001 President and Fellows of Harvard College.
    - Hughes, R.L. (2005). What is Strategic Leadership (Chapter 1), Becoming a strategic leader: Your role in your organization's enduring success. San Francisco: Jossey-Bass. Copyright © 2005 John Wiley & Sons, Inc.
    - Panagiotou, G. (2003). Bringing SWOT into Focus, Business Strategy Review, 14(2), 8–10. Copyright © 2003 Blackwell Publishing Ltd.
    - Weitzel, W., & Jonsson, E. (1989). Decline in Organizations: A Literature Integration and Extension, Administrative Science Quarterly, 34, 91–109. Copyright © 1989 Cornell University.

Activities

- Familiarize yourself with the course website by reviewing the **Start Here** section of the course.
- Review the **Outline** and **Assessments** sections on the course website to learn about course expectations, assessments, and due dates.
- Confirm your access to the course reserve materials by selecting **Ares** on the navbar.
- Submit the *Tell Me About Yourself* form to the **Dropbox**.

Assessments

- Begin working on the **Integrative Project**.

Unit 02: The Planned Approach to Change

Week 2 –

Readings

- CourseLink Website: Unit 02 Content
- Ares:
  - Beer, M., & Nohria, N. (2000). Cracking the code of change. HBR's 10 Must Reads on Change, 88.
  - Cummings, T. G. Chapter 7: The Practice of Organization Development.
  - Burnes, B. (2004). Kurt Lewin and the Planned Approach to Change: A Re-appraisal, Journal of Management Studies, 41(6), 977–1002. Copyright © 2004 Blackwell Publishing Ltd.
  - Thomas, J. Force Field Analysis: A New Way to Evaluate Your Strategy.
  - Kotter, J.P. (2007). Leading Change: Why Transformation Efforts Fail, Harvard Business Review, 85(1), 96–103. Copyright © 2007 Harvard Business Review.

Assessments

- Complete the **Weekly Integrative Project Assignment**.

Unit 03: The Emergent Approach to Change

Week 3 –

Readings

- CourseLink Website: Unit 03 Content
- Ares:

- Wheatley, M.J. (2006). Newtonian Organizations in a Quantum Age, Leadership in the new science. San Francisco: Berret-Koehler Publishers Inc. Copyright © 2006 Berret-Koehler Publishers Inc.
- Tetenbaum, T.J. (1998). Shifting Paradigms: From Newton to Chaos, Organizational Dynamics, 26(4), 21–32. Copyright © 1998 Elsevier Inc.
- Plowman, D.A., Solansky, S., Beck, T.E., Baker, L., Kulkarni, M., & Travis, D.V. (2007). The Role of Leadership in Emergent, Self-Organization, Leadership Quarterly, 18, 341–356. Copyright © 2007 Elsevier Inc.
- Weick, K. E. (2000). Emergent change as a universal in organizations. Breaking the code of change, 223-241.

Assessments

- Complete the **Weekly Integrative Project Assignment**.
- **Participation #1 (Self-Assessment)**
  Due:

Unit 04: Sources of and Approaches to Dealing with Resistance

Week 4 –

Readings

- CourseLink Website: Unit 04 Content
- Ares:
  - Elrod II, P.D., & Tippett, D.D. (2002). The “Death Valley” of Change, Journal of Organizational Change Management, 15(3), 273–291. Copyright © 2002 MCB UP Ltd.
  - Erwin, D. G., & Garman, A. N. (2010). Resistance to organizational change: linking research and practice. Leadership & Organization Development Journal, 31(1), 39-56.
  - Kotter, J. P., & Schlesinger, L. A. (2008). Choosing strategies for change. Harvard business review, 130-139
  - Ford, J. D., Ford, L. W., & D'Amelio, A. (2008). Resistance to change: The rest of the story. Academy of management Review, 33(2), 362-377.

Assessments

- Complete the **Weekly Integrative Project Assignment**.
- **Comparison & Contrast**
  Due:

Unit 05: Points of Leverage

Week 5 –

Readings

- CourseLink Website: Unit 05 Content
- Ares:
  - Burke, W.W. (2002). The Burke-Litwin Causal Model of Organizational Performance and Change (Chapter 9), Organizational Change: Theory and Practice. Thousand Oaks: Sage Publications. Copyright © 2002 Sage Publications.
  - Coghlan, D. (2000). Interlevel dynamics in clinical inquiry. Journal of Organizational Change Management, 13(2), 190-200.
  - Krackhardt, D, & Hanson, J.R. (1993). Informal Networks: The Company, Harvard Business Review, 71(4), 104–111. Copyright © 1993 President and Fellows of Harvard College.
  - Nadler, D. A., & Tushman, M. L. (1980). A model for diagnosing organizational behavior. Organizational Dynamics, 9(2), 35-51.
  - Mark, K. (2006). Leading Change at SJHC and LHSC: Burr Under the Saddle or a Grain of Sand in the Oyster, Ivey Management Case Study. Copyright © 2006, Ivey Management Services. [under Case Study]
  - Built to Change [video; under Additional Resources]

Assessments

- Complete the **Weekly Integrative Project Assignment**.
- Begin working on **Case Study (Group Project)**.

Unit 06: Integration/Contingency

Week 6 –

Readings

- CourseLink Website: Unit 06 Content
- Ares:
  - Dunphy, D., & Stace, D. (1993). The Strategic Management of Corporate Change, Human Relations, 46(8), 905–920. Copyright © 1993 The Tavistock Institute.
  - Hailey, V.H., & Balogun, J. (2002). Devising Context Sensitive Approaches to Change: The Example of Glaxo Wellcome, Long Range Planning, 35(2), 153–178. Copyright © 2002 Elsevier Science Ltd.

- Palmer, I., & Dunford, R. (2008). Organizational change and the importance of embedded assumptions. British Journal of Management, 19(s1).
- By, R. T., Hughes, M., & Ford, J. (2016). Change leadership: Oxymoron and myths.

Assessments

- Complete the **Weekly Integrative Project Assignment**.
- **Case Study (Group Project)**
  Due: Sunday, April 17 by 11:59 pm ET
- **Peer Evaluation (Case Study)**
  Due:

Unit 07: Changing Quietly

Week 7 –

Readings

- CourseLink Website: Unit 07 Content
- Ares:
  - Dutton, J.E., Ashford, S.J., O'Neill, R.M., & Lawrence, K.A. (2001). Moves that Matter: Issue Selling and Organizational Change, Academy of Management Journal, 44(4), 716–736. Copyright © 2001 Academy of Management Journal.
  - Meyerson, D. E. (2001). Radical change, the quiet way. HBR's 10 Must Reads on Change, 39.
  - Friedman, V. J. (2002). The individual as agent of organizational learning. California Management Review, 44(2), 70-89.
  - Frohman, A. L. (1997). Igniting organizational change from below: The power of personal initiative. Organizational Dynamics, 25(3), 39-53.

Assessments

- **Integrative Project**
  Due:
- **Participation #2 (Self-Assessment)**
  Due:

Assessments

The grade determination for this course is indicated in the following table. A brief description of each assessment is provided below. Select **Content** on the navbar to locate **Assessments** in the table of contents panel to review further details of each assessment. Due dates can be found under the Schedule heading of this outline.

Table 1: Course Assessments

Assessment Item	**Weight**
Compare and Contrast	20%
Integrative Project	40%
Participation (self-assessments)	10%
Case Study (group project)	30%
Total	**100%**

Assessment Descriptions

Compare and Contrast

In this project, you are asked to compare and contrast the planned and emergent approaches to change management. Your objective in this report is to provide an analysis of the key concepts, issues, ideas, etc. that are similar and different between the planned and emergent approaches. Your primary focus should be on a critical analysis of the conceptual underpinnings of the two approaches. Your aim is to demonstrate that you understand and appreciate the key concepts within the two approaches well enough that you are able to identify in what ways they are comparable, and in what ways they are at variance with one another.

Integrative Project

Each week you will have a task to perform that will help you apply the week's material. These tasks will culminate in your Integrative Project. The focus of the project is on a change that you believe needs to be made in your organization in order for it to operate successfully for the foreseeable future (think three to five years out). Each week you will apply the readings to this potential change as a means of helping you "get your head around" the material we'll be covering (this may also help you develop a plan of action if you are currently planning such a change at work).

Participation (self-assessments)

Although not the primary focus in this course, you are expected to participate in the General Discussions on an ongoing basis. You should expect to actively participate at least three times per week. More on-line participation may be required to complete specific projects.

You will be asked to submit a self-assessment of your participation in the General Discussions twice throughout the course – once in week 3 and once in week 7. In these self-assessments, you will not consider the frequency, but the level (i.e., quality) of your contribution to the discussions).

Case Study (group project)

The purpose of the Case Study (group project) is to further promote your appreciation of the value of the course material by discussing it with the express purpose of addressing a real leadership challenge pertaining to organizational change. Along with your group members, your job in the case will be to analyze the problems and develop an action plan to produce needed changes. The case study is available through **Ares**.

Course Technologies and Technical Support

CourseLink System Requirements

You are responsible for ensuring that your computer system meets the necessary system requirements. Use the browser check tool to ensure your browser settings are compatible and up to date. (Results will be displayed in a new browser window).

https://opened.uoguelph.ca/student-resources/system-and-software-requirements

https://courselink.uoguelph.ca/d2l/systemCheck

Zoom System Requirements

This course may use **Zoom** as a video communication tool. A Webcam, a microphone to record video, and headphones/speakers to play back the recording are also needed. In order to use Zoom, you must meet the following technical requirements:

1. An internet connection – broadband wired or wireless (3G or 4G/LTE)
2. Speakers and a microphone – built-in or USB plug-in or wireless Bluetooth
3. A webcam or HD webcam - built-in or USB plug-in
4. Supported mobile platforms: Android 4.4 or later and iOS 10.0 or later.

Technical Skills

As part of your online experience, you are expected to use a variety of technology as part of your learning:

- Manage files and folders on your computer (e.g., save, name, copy, backup, rename, delete, and check properties);
- Install software, security, and virus protection;
- Use office applications (e.g., Word, PowerPoint, Excel, or similar) to create documents;
- Be comfortable uploading and downloading saved files;
- Communicate using email (e.g., create, receive, reply, print, send, download, and open attachments);
- Navigate the CourseLink learning environment and use the essential tools, such as **Dropbox**, **Discussions**, and **Grades** (the instructions for this are given in your course);
- Access, navigate, and search the Internet using a web browser (e.g., Firefox, Internet Explorer); and
- Perform online research using various search engines (e.g., Google) and library databases.

Technical Support

If you need any assistance with the software tools or the CourseLink website, contact CourseLink Support.

CourseLink Support
University of Guelph
Day Hall, Room 211
Email: courselink@uoguelph.ca
Tel: 519-824-4120 ext. 56939
Toll-Free (CAN/USA): 1-866-275-1478

Walk-In Hours (Eastern Time):
Monday thru Friday: 8:30 am–4:30 pm

Phone/Email Hours (Eastern Time):
Monday thru Friday: 8:30 am–8:30 pm
Saturday: 10:00 am–4:00 pm
Sunday: 12:00 pm–6:00 pm

Course Specific Standard Statements

Acceptable Use

The University of Guelph has an Acceptable Use Policy, which you are expected to adhere to.

https://www.uoguelph.ca/ccs/infosec/aup

Communicating with Your Instructor

During the course, your instructor will interact with you on various course matters on the course website using the following ways of communication:

- **Announcements:** The instructor will use **Announcements** on the Course Home page to provide you with course reminders and updates. Please check this section frequently for course updates from your instructor.
- **Ask Your Instructor Discussion:** Use this discussion forum to ask questions of your instructor about content or course-related issues with which you are unfamiliar. If you encounter difficulties, the instructor is here to help you. Please post general course-related questions to the discussion forum so that all students have an opportunity to review the response. To access this discussion forum, select **Discussions** from the **Tools** dropdown menu.
- **Email:** If you have a conflict that prevents you from completing course requirements, or have a question concerning a personal matter, you can send your instructor a private message by email. The instructor will respond to your email within 48 to 72 hours.
- **Online meetings:** If you have a complex question you would like to discuss with your instructor, you may book an online meeting. Online meetings depend on the availability of you and the instructor, and are booked on a first come first served basis.

Netiquette Expectations

For online courses, the course website is considered the classroom and the same protections, expectations, guidelines, and regulations used in face-to-face settings apply, plus other policies and considerations that come into play specifically because these courses are online.

Inappropriate online behaviour will not be tolerated. Examples of inappropriate online behaviour include:

- Posting inflammatory messages about your instructor or fellow students;
- Using obscene or offensive language online;
- Copying or presenting someone else's work as your own;
- Adapting information from the Internet without using proper citations or references;
- Buying or selling term papers or assignments;
- Posting or selling course materials to course notes websites;
- Having someone else complete your quiz or completing a quiz for/with another student;

- Stating false claims about lost quiz answers or other assignment submissions;
- Threatening or harassing a student or instructor online;
- Discriminating against fellow students, instructors, and/or TAs;
- Using the course website to promote profit-driven products or services;
- Attempting to compromise the security or functionality of the learning management system;
- Sharing your username and password; and
- Recording lectures without the permission of the instructor.

Submission of Assignments to Dropbox

All assignments for this course should be submitted electronically via the online **Dropbox** tool. When submitting your assignments using the **Dropbox** tool, do not leave the page until your assignment has successfully uploaded. To verify that your submission was complete, you can view the submission history immediately after the upload to see which files uploaded successfully. The system will also email you a receipt. Save this email receipt as proof of submission.

Be sure to keep a back-up copy of all of your assignments in the event that they are lost in transition. In order to avoid any last-minute computer problems, your instructor strongly recommend you save your assignments to a cloud-based file storage (e.g., Google Docs), or send to your email account, so that should something happen to your computer, the assignment could still be submitted on time or re-submitted.

It is your responsibility to submit your assignments on time as specified on the Schedule. Be sure to check the technical requirements and make sure you have the proper computer, that you have a supported browser, and that you have reliable Internet access. Remember that **technical difficulty is not an excuse not to turn in your assignment on time.** Don't wait until the last minute as you may get behind in your work.

If, for some reason, you have a technical difficulty when submitting your assignment electronically, please contact your instructor or CourseLink Support.

https://support.opened.uoguelph.ca/contact

Submitting the Wrong Version of Assignments to the Dropbox

When people submit assignments to **Dropbox**, they sometimes subsequently realize that they submitted the wrong version (usually an older draft). They then submit the correct version and end up with two copies of the assignment in **Dropbox**. When this happens, I often end up reading and grading the wrong version. If you submit the wrong version of any assignments, please e-mail CourseLink Support immediately to have the faulty assignment removed. When you e-mail CourseLink Support, you must Cc me on the message because tech support requires my approval to delete assignments. Please

note that if I read the wrong version of an assignment, the grade assigned to the version I have read will be the grade awarded.

Late Policy

All assignments must be submitted on the due date unless otherwise specified. If assignments are handed in late, 20% of the total marks will be deducted for every day they are late (including weekends). The end of the day is 5:00 pm ET. Assignments handed in after 5:00 pm ET on any given day will be considered to be another day late.

Extensions will be considered for medical reasons or other extenuating circumstances. If you require an extension, discuss this with the instructor as soon as possible and well before the due date. Barring exceptional circumstances, extensions will not be granted once the due date has passed. These rules are not designed to be arbitrary, nor are they inflexible. They are designed to keep you organized, to ensure that all students have the same amount of time to work on assignments, and to help to return marked materials to you in the shortest possible time.

Obtaining Grades and Feedback

Unofficial assessment marks will be available in the **Grades** tool of the course website.

Your instructor will have grades posted online within 2 weeks of the submission deadline, if the assignment was submitted on time. Once your assignments are marked you can view your grades on the course website by selecting **Grades** from the **Tools** dropdown menu on the navbar. Your course will remain open to you for one year following the end of your program.

Final grades will be available at the end of the semester. Students can access their final grade by logging into WebAdvisor (using your U of G central ID).

https://webadvisor.uoguelph.ca

Regrading

If you get an assignment back, disagree with the grade, and would like to have it re-graded, please contact me within five days of the grades being posted. In your message, please avoid asking any variant of “where did I lose marks?” That is too broad a question for me to answer effectively. If you contact me about a lower-than-expected grade (nobody ever e-mails to say their grade is too high), you undoubtedly feel that specific issues/ points/ arguments/ etc. that you included were, perhaps, overlooked. Therefore, please specify clearly and precisely what these points are and why you think your assignment deserves to be reconsidered. Note that when I re-read an assignment, the entire assignment gets re-graded. Thus, regrading an assignment can result in the grade increasing or decreasing. I do read the assignments carefully the first time, so grade changes are rare. You are, of course, always welcome to discuss details of assignments with me without requesting regrading.

Please note that I can only evaluate your assignments based on what is written in them. A common reason for re-grade requests is that students indicate that they “meant to

say" something that didn't come across clearly enough in the report. However, I can't evaluate anyone on what they "meant to say", only on what they "did" say. So, proofread your assignments carefully. The quality of your writing counts (directly and indirectly).

Rights and Responsibilities When Learning Online

The course website is considered the classroom and the same protections, expectations, guidelines, and regulations used in face-to-face settings apply, plus other policies and considerations that come into play specifically because these courses are online.

For more information on your rights and responsibilities when learning in the online environment, visit Rights and Responsibilities.

http://opened.uoguelph.ca/student-resources/rights-and-responsibilities

---

Program Specific Standard Statements

Equity, Diversity, and Inclusion

At the Lang School of Business and Economics, we are committed to developing leaders with a social conscience, an environmental sensibility, and a commitment to their communities. A core tenet within this vision is that diversity is a strength with which we can experience greater connection and understanding.

As such, we affirm the importance and shared responsibility of our students, faculty, and staff creating and promoting equity and inclusion within our learning spaces. Creating these kinds of learning cultures is a process, not a destination; it requires ongoing willingness on the part of each person to thoughtfully and critically listen, unlearn, learn, and engage as they are exposed to a multitude of perspectives and lived experiences. We encourage dialogues between students and instructors to address and advance opportunities for fostering greater diversity and inclusion in the learning environment. Openness to conversations with each other enables us to reflect and grow as we learn from one another respectfully and holistically.

As a department that is training the professionals of the future, we expect our learning spaces to abide by all institutional policies and guidelines, in particular those outlined by the Office of Diversity and Human Rights and the University of Guelph Human Rights Policy. Discrimination and harassment, as defined by our policies, will not be tolerated. Individuals should inform the appropriate party as per University policies if they experience any such behaviours.

https://www.uoguelph.ca/diversity-human-rights/human-rights-policy-and-procedures

University Standard Statements

University of Guelph: Graduate Policies

As a student of the University of Guelph, it is important for you to understand your rights and responsibilities and the academic rules and regulations that you must abide by. Consult the Graduate Calendar for the rules, regulations, curricula, programs and fees for current and previous academic years.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Email Communication

As per university regulations, all students are required to check their uoguelph.ca e-mail account regularly: e-mail is the official route of communication between the University and its students.

When You Cannot Meet Course Requirements

When you find yourself unable to meet an in-course requirement due to illness or compassionate reasons, please advise your course instructor (or designated person such as a teaching assistant) **in writing**, with your name, ID number and email contact.

Review the Graduate Calendar for information on regulations and procedures for Academic Consideration.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Drop Date

The last date to drop one-semester courses, without academic penalty, is indicated in the Schedule of Dates section of the Graduate Calendar. Review the Graduate Calendar for regulations and procedures for Dropping Courses.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Copies of Out-of-Class Assignments

Keep paper and/or other reliable back-up copies of all assignments: you may be asked to resubmit work at any time.

Accessibility

The University of Guelph is committed to creating a barrier-free environment. Providing services for students is a shared responsibility among students, faculty and administrators. This relationship is based on respect of individual rights, the dignity of the individual and the University community's shared commitment to an open and supportive learning environment.

Students requiring service or accommodation, whether due to an identified, ongoing disability or a short-term disability should contact Accessibility Services as soon as possible.

For more information, contact Accessibility Services at 519-824-4120 ext. 56208, email Accessibility Services or visit the Accessibility Services website.

accessibility@uoguelph.ca

https://wellness.uoguelph.ca/accessibility/

Academic Misconduct

The University of Guelph is committed to upholding the highest standards of academic integrity and it is the responsibility of all members of the University community – faculty, staff, and students – to be aware of what constitutes academic misconduct and to do as much as possible to prevent academic offences from occurring. University of Guelph students have the responsibility of abiding by the University's policy on academic misconduct regardless of their location of study; faculty, staff and students have the responsibility of supporting an environment that discourages misconduct. Students need to remain aware that instructors have access to and the right to use electronic and other means of detection.

The Academic Misconduct Policy is detailed in the Graduate Calendar.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Copyright

Content within this course is copyright protected. Third party copyrighted materials (such as book chapters and articles) have either been licensed for use in this course, or have been copied under an exception or limitation in Canadian Copyright law.

The fair dealing exemption in Canada's Copyright Act permits students to reproduce short excerpts from copyright-protected materials for purposes such as research, education, private study, criticism and review, with proper attribution. Any other copying, communicating, or distribution of any content provided in this course, except as permitted by law, may be an infringement of copyright if done without proper license or the consent of the copyright owner. Examples of infringing uses of copyrighted works would include uploading materials to a commercial third party web site, or making paper or electronic reproductions of all, or a substantial part, of works such as textbooks for commercial purposes.

Students who upload to CourseLink copyrighted materials such as book chapters, journal articles, or materials taken from the Internet, must ensure that they comply with Canadian Copyright law or with the terms of the University's electronic resource licenses.

For more information about students' rights and obligations with respect to copyrighted works, review Fair Dealing Guidance for Students.

http://www.lib.uoguelph.ca/sites/default/files/fair_dealing_policy_0.pdf

Grades

The assignment of grades at the University of Guelph is based on clearly defined standards which are published in the Graduate Calendar for the benefit of faculty and students**.** In courses, which comprise a part of the student's program, standings will be reported according to the following schedule of grades and will use the following definitions for each of the numerical grade range (letter grades):

Table 2: Grade Interpretation

Percentage Grade	Letter Grade	Description
90-100	A+	**Outstanding.** The student demonstrated a mastery of the course material at a level of performance exceeding that of most scholarship students and warranting consideration for a graduation award.
80-89	A- to A	**Very Good to Excellent.** The student demonstrated a very good understanding of the material at a level of performance warranting scholarship consideration.
70-79	B	**Acceptable to Good.** The student demonstrated an adequate to good understanding of the course material at a level of performance sufficient to complete the program of study.
65-69	C	**Minimally Acceptable.** The student demonstrated an understanding of the material sufficient to pass the course but at a level of performance lower than expected from continuing graduate students.
0-64	F	An inadequate performance.

Further information on the Grades Schedule and Grade Interpretation can be found in the Graduate Calendar.

https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-as-gradesch.shtml

https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-as-gradeint.shtml

Graduate Student Responsibilities

From the choice of Advisor, choice of research project and through to degree completion, graduate students must recognize that they carry the primary responsibility for their success. The responsibilities assigned to Advisors, Advisory Committees and Departments provide the framework within which students can achieve success. Students should take full advantage of the knowledge and advice that the Advisor and Advisory Committee have to offer and make the effort to keep the lines of

communication open. The Graduate Student Responsibilities are located in the Graduate Calendar.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

General Regulations

Graduates students are expected to be familiar with the General Regulations in the Graduate Calendar, including those related to university-wide policies on admission, registration, graduation, theses, fees and other subjects of importance to graduate students.

https://www.uoguelph.ca/registrar/calendars/graduate/current/

Plagiarism Detection Software

Students should be aware that faculty have the right to use software to aid in the detection of plagiarism or copying and to examine students orally on submitted work. For students found guilty of academic misconduct, serious penalties, up to and including suspension or expulsion from the University can be imposed.

Recording of Materials

Presentations which are made in relation to course work—including lectures—cannot be recorded or copied without the permission of the presenter, whether the instructor, a classmate or guest lecturer. Material recorded with permission is restricted to use for that course unless further permission is granted.

Disclaimer

Please note that the ongoing COVID-19 pandemic may necessitate a revision of the format of course offerings, changes in classroom protocols, and academic schedules. Any such changes will be announced via CourseLink and/or class email.

This includes on-campus scheduling during the semester, mid-terms and final examination schedules. All University-wide decisions will be posted on the COVID-19 website and circulated by email.

https://news.uoguelph.ca/2019-novel-coronavirus-information/

Illness

Medical notes will not normally be required for singular instances of academic consideration, although students may be required to provide supporting documentation for multiple missed assessments or when involving a large part of a course (e.g., final exam or major assignment).

Covid-19 Safety Protocols

For information on current safety protocols, follow these links:

- **How U of G Is Preparing for Your Safe Return**
- **Guidelines to Safely Navigate U of G Spaces**

Please note, these guidelines may be updated as required in response to evolving University, Public Health or government directives.

https://news.uoguelph.ca/return-to-campuses/how-u-of-g-is-preparing-for-your-safe-return/

https://news.uoguelph.ca/return-to-campuses/spaces/#ClassroomSpaces

MGMT*6400 Project Management
Course Outline

Pre-Requisite(s): None
Co-Requisite(s): None
Restriction(s): Lang graduate students only
Method of Delivery: Online DE
Course Website Access Date: TBD
Course Start Date: TBD
Course End Date: TBD
Final Exam: There is no final exam in this course.

Calendar Description

This course provides students with an understanding of the concepts, principles, and practices for project management. It introduces an understanding and appreciation of the importance of managing projects, project teams, the project management systems and tools, the various components of the project management process, and professional codes of conduct and ethics. The emphasis is on the techniques most frequently used in the context of, both internal and external organizational roles of a project manager.

Indicative Content

Module	Topic	Readings
1	Introduction to the course and introduction to Project Management (overview).	Chapter 1 and 2
2	Project definition and project scope	Chapter 3 and 4
3	Ideation, problem solving, scheduling and estimating resources.	Chapters 5 and 6
4	Agile Project Management and practices and Project Risk Management	Chapter 15 Chapter 7
5	Managing resources and project crashing Project Management Metrics	Chapters 8, 9 and 13

6	The soft skills in Project Management	Chapters 10, 11, and 12
7	International Project Management Project Closure	Chapters 14 and 16

Course Learning Outcomes

Upon successfully completing this course, students will be able to:

Critical and Creative Thinking:

1. Evaluate a project based on the concepts in the Project Management Body of Knowledge.
2. Optimize a project while managing the triple constraints of time, cost, and scope
3. Apply the Project Management Body of Knowledge for planning, executing, controlling, and closing a project through its lifecycle
4. Track Project progress and performance and manage changes to the project baseline

Professional and Ethical Behaviour:

5. . Use negotiation skills in initiating and managing changes to project scope
6. Examine team effectiveness, and team leadership
7. Identify and analyse the ethical considerations implicit in managing projects, including the potential effects on project owner, sponsor, and users

Literacy

8. Identify and analyze roles and responsibilities in projects and contemporary approaches to project management.
9. Systematically review the literature on project management

Communication:

10. Report project progress effectively to project stakeholders in oral and written format
11. Create project management documents related to project scope, plan, schedule, risk, communication, quality, and project closing.

Course Assessment

All assignments should be included in the e-portfolio

			Related Learning Outcomes
Assessment 1	30%	Content Quizzes 3 X 10%	1-4
Assessment 2	50%	Applied Project	5-9
Assessment 3	20%	Individual Essay	8-11

Assessment 1 - Weekly Quizzes: every week you will be expected to complete a quiz on the material from that week's reading(s). This quiz may be a combination of multiple choice, true/false, or short answer questions. Each quiz is expected to be completed for an individual score of 3% per quiz. If you miss the deadline for the quiz, then you lose the marks for that quiz.

Assessment 2 - Applied Project - Group Assignment Details

Task	Description	% of total grade
Scheme A Case Assessment (5)	Formative Cases	5 x 2% = 10% (group)
Scheme B Project Update Meetings (6)	Meetings in-class	6 x 1.5% = 9% (group)
Scheme C Project - Scoping Review	Contract + 3 updates + Portfolio + pstn	2%+3x2%+15%+5% = 28% (group)
Scheme D PEAR Assessment	Personal reflection & peer evaluation	5% (individual)

Applied Project: the applied project consists of formative case assessments that will help you in your own team's project development and on the submission of project versions all the way to a final presentation and a final project portfolio submission.

The class will be randomly divided into teams of approximately 4 students each. Each team will be given a project. For this assignment the instructor will play the role of the project owner and the sponsor. I will provide the project charter for the project. Each team must define the project scope, prepare a project plan including a work break down structure and estimation, a risk management plan, a communication plan, and execute the project to deliver the expected final product.

There will be formative assignments and progress plan updates required weekly; meetings are designed to lead progressively towards the final project report. Activities in each week build on assignments completed in the previous weeks.
The formative case assignments will be provided by the instructor in the week prior to their submission deadline. They will be based on cases designed to address the five

topics of Project Scope, Project Management Risk, Project Communication, Project Metrics, and Project Closure. Each case assignment is a group submission with a grade of 2% of overall mark per case for a total course weight of 10% and it will be applied as a group grade.

Individual Essay - Project leadership essay: In this assignment students are required to demonstrate their ability to use leadership theories in project management. You will be assigned a leadership theory and in an essay of maximum 2000 words, excluding references, double spaced, explain how that theory is used in the project management literature, and how that theory can help you develop your leadership skills. The essay should have an introduction that introduces the theory. It should use at least 5 academic papers (peer-reviewed publications) that have used that theory. Include an additional 500-1000 words about your own leadership experiences and how this leadership theory applies (or not) to your experiences.

To encourage you to not wait too long before working on the essay, I will be happy discuss your assignments until the end of class of the week before they are due. I won't discuss or review the assignments after the end of that class.

Required Reading Materials:

ISE Project Management: The Managerial Process (8th Ed.) Erik W. Larson and Clifford F. Gray Print: ISBN 978 126 0579 567