Toronto Metropolitan University

Graduate & Postdoctoral Studies

MASTER OF CYBERSECURITY (MC)

CURRICULUM

[First offered Fall 2025]

Master of Cybersecurity

DEGREE REQUIREMENTS		**Credits**
CB8101	Fund. of Info Assurance	1
CB8102	Cybersecurity Risk Management	1
CB8103	Cyber FWs, Gov., and Compliance	1
CB8104	Security Architecture	1
CB8105	Fundamentals of Security Tech.	1
Three credits from the Electives List		3

ELECTIVES		
CB8201	Privacy, Law and Ethics	1
CB8202	Sec. Ops. Bus. Cont. Dis. Rec.	1
CB8203	Simulations in the Cyber Range	1
CB8204	Software Development Security	1
CB8205	Network Security	1
CB8206	Applied Cryptography	1

COURSE LISTING

CB8101 Fundamentals of Information Assurance

This course provides an overview of the managerial processes of cybersecurity that are fundamental to an enterprise cybersecurity program and discusses how they can best be implemented and maintained with best practices. It focuses on the principles of security management, security policy, human resources security, information management, physical and infrastructure security, supply chain management as well as security audit. The course will also discuss securing the past, present and future of an enterprise by means of appropriate security controls, 1 Credit

CB8102 Cybersecurity Risk Management

This course gives an overview of internal and external cybersecurity risks to organizations and how they can be managed. It outlines the tactics, techniques, and procedures of threat actors, as well as their motivations and intent. It covers risk assessment, analysis, management, and treatment—as well as the frameworks, international standards, and guidelines that regulate these practices. It explains methods of equipping organizations to make informed business risk decisions, depending on their industries and the maturity level of their security programs. 1 Credit

CB8103 Cyber FWs, Gov., and Compliance

This course gives an overview of the regulatory and industry-driven frameworks that govern an organization's cybersecurity program. Topics covered include the governance, risk, and compliance (GRC) concepts that apply to cybersecurity; the role of a Chief Information Security Officer (CISO), including its historical evolution; the implementation of cybersecurity governance within a business risk program; and methods of achieving cybersecurity compliance within an IT risk management program. 1 Credit

CB8104 Security Architecture

This course will explore the concept of security architecture in a time of change. Where traditional security architectures involved protecting the "perimeter" of the organization's network, many organizations are moving to cloud-hosted services. The course will cover the security architect's role in assessing what information can and should be stored in the cloud, and in setting up security infrastructure—as it applies to IT networks, data protection, security monitoring, and auditing. 1 Credit

CB8105 Fundamentals of Security Technologies

This course provides an overview of the technology that is fundamental to an organization's cybersecurity program and considers how it can best be deployed. It focuses on the principles of identity security and access management (IAM) as well as the protection of data, the world's modern currency. Concepts covered include role-based access, access modeling, trust models for access control, privileged account management, credential management, and authentication. The course will also discuss the way innovation works in cybersecurity. 1 Credit

CB8201 Privacy, Law and Ethics

This course examines the legal and ethical aspects of the relationship between privacy and cybersecurity. The legal and ethical obligations of cybersecurity professionals, and of organizations, with respect to privacy and personal information protection are explored. Key conceptual ideas, such as treating privacy and security as a "zero-sum" game, privacy by design and by default, and ethical programming are reviewed and discussed. No prior knowledge of law or ethics is required. 1 Credit

CB8202 Sec. Ops Business Cont. Disaster Recovery

Principles and practices of enterprise continuity and disaster recovery are presented with respect to cybersecurity operations within an enterprise framework, using the elements of cyber resilience: prepare/identify, protect, detect, respond, and recover as teaching principles. 1 Credit

CB8203 Cyber Simulations in the Cyber Range

This course provides an overview and survey of multiple cyber security frameworks and implements these frameworks practically in the Catalyst Cyber Range: a unique cybersecurity training and testing platform that provides immersive and ultra-realistic experiential learning opportunities. The Catalyst Cyber Range features a customizable technology platform and an array of real-world cybersecurity scenarios. This course focuses on the technical areas of the enterprise, incident response, penetration testing, cybersecurity operations, digital forensics and network security. The NIST Cybersecurity, Mitre ATT&CK and Cyber Kill Chain frameworks are applied in multiple cyber scenarios. 1 Credit

CB8204 Software Development Security

This course provides an overview of Software security that along with cryptography, access control and security protocols is fundamental to an organization's cybersecurity program. The course focuses on the main sources of insecurity in software including software flaws as unintentional source of insecurity and malware as the intentional source, and discusses how the flaws and malware can be exploited through software reverse engineering (SRE). The course also covers main concepts of security in operating systems (OS) including security. 1 Credit

CB8205 Network Security

With the growing use of online distributed processing, secure access to computing infrastructure is of paramount importance that can be ensured by the network security. This course explores concepts, tools and services necessary to achieve network security design. It discusses authentication and IPSec VPN including site-site VPN. It explains protection of the network through access control and firewall. The modern networks face enormous attacks by intruders... The course assumes a working knowledge of cryptography. 1 Credit

CB8206 Applied Cryptography

This course provides a rigorous treatment of modern applied cryptography, emphasizing both theoretical foundations and practical applications. Topics include advanced symmetric and asymmetric cryptosystems, cryptographic hash functions, message authentication codes, digital signatures, key management protocols, and advanced cryptographic protocols such as zero-knowledge proofs and secure multi-party computation. The course also explores real-world applications and current research trends in areas such as blockchain technologies, privacy-preserving computation, and post-quantum cryptography. 1 Credit

---