CIBC MELLON

GOVERNANCE AND RISK CULTURE:

A FRAMEWORK FOR EFFECTIVE OVERSIGHT

DECEMBER 2025

CONTRIBUTORS

KELLY HASTINGS
Chief Risk Officer

ROB FISCHER
Chief Compliance Officer

BEN KENTON
Chief Internal Auditor

TIZIANA MANCINI
Vice President, Operational Risk

JEROME MONTPETIT
Vice President,
Credit and Market Risk

KEVIN KONDO
Vice President, Information
Technology Enterprise Resilience

CAROLIN BROADBRIDGE
Assistant Vice President,
Third Party Governance

Integrity, risk awareness and ethical conduct form the foundation of CIBC Mellon's corporate culture. As an organization focused on operational transaction processing, we recognize that diligent attention to organizational risk, governance, transparency and personal accountability are at the centre of maintaining our clients' trust. Clients take assurance from CIBC Mellon's robust risk and internal control framework, which enables independent identification, assessment, monitoring and reporting of risks across the enterprise.

EXPLORE WITH US

We would be pleased to discuss these themes further, including exploring them in the context of our ongoing Canadian and global research efforts. Please do not hesitate to contact your client manager to arrange a discussion.

CIBC MELLON'S COMMITMENT TO MAINTAINING A STRONG RISK MANAGEMENT FRAMEWORK

CIBC Mellon plays a critical role in supporting clients, providing a solid infrastructure for Canada's capital markets and recognizes that its financial stability through market cycles is essential. Accordingly, CIBC Mellon is committed to maintaining a strong balance sheet that is characterized by superior asset quality. Our risk management framework is designed to ensure that the business remains aligned with its risk appetite statement.

KEY COMPONENTS OF CIBC MELLON'S RISK MANAGEMENT FRAMEWORK

1. **Confirming appropriate limits are in place to govern CIBC Mellon's risk-taking activities across all risk types**
2. **Incorporating risk appetite principles into strategic decision-making processes**
3. **Monitoring and reporting key risk metrics to Senior Management and CIBC Mellon's Board of Directors**
4. **Providing a continuous and forward-looking capital planning process to support CIBC Mellon's risk-taking activities**

CIBC Mellon monitors its risk across a wide array of risk categories. Often the main focus of managing operational risks in a given organization is to prepare for and react to significant events. While institutions must be well prepared for these high-profile events, the majority of operational risk comes from day-to-day business processing. These operational risks must be managed considering the processes, people and systems that are part of the risk framework.

CIBC Mellon's Risk Management Framework promotes the identification, measurement, management, monitoring and escalation of all credit, market, information and operational risks across the enterprise. This allows all business units, including CIBC Mellon's governance partners and risk management group, to assure the Board of Directors, shareholders, and regulators that there is a strong risk management structure at CIBC Mellon.

The structure of the framework, in conjunction with the oversight provided by the Governance partners, the Risk Committees and Management, ensures that CIBC Mellon manages risk to remain aligned with the risk appetite statement.

OUR GOVERNANCE COMMITTEES

AML Committee	The AML Committee provides oversight on matters relating to CIBC Mellon's AML Program.
Asset and Liability Committee (ALCO)	ALCO is responsible for setting the risk tolerance and associated market risk limits.
Business Acceptance Committee (BAC)	All business for new clients and all new business for existing clients must be approved through the BAC to ensure new business meets our standards, and protects our reputation for stakeholders and clients.
Core Tax and Tax Tribunal	The Core Tax Team is responsible for overseeing, promoting and sustaining an operational tax control environment that is effective in mitigating regulatory, financial, reputational and other risks associated to complying with CIBC Mellon's regulatory tax requirements. The Tax Tribunal is responsible for reviewing and making decisions on any requested exceptions to the tax procedures and company policies.
Credit Risk Committee	The Credit Risk Committee recommends the counterparty and group limits in the Capital Markets Limits Policy, which is approved annually by the Board of Directors.
Executive Portfolio Steering Committee (EPSC)	EPSC's primary focus is to ensure that there is an appropriate assessment of all new initiatives.
Information Management Committee (IMC)	The IMC has responsibility for information risk management.
Operational Risk Committee (ORC)	The ORC is responsible for completing a formal review of the operational risk management practices in each business unit.
Third-Party Governance Committee	The Third-Party Governance Committee provides assurance that a strong third-party management culture exists within CIBC Mellon and that third-party risks being assumed are consistent with CIBC Mellon's risk appetite.
Trustee Governance Committee	The Trustee Governance Committee provides oversight of all relationships where CIBC Mellon acts as a Trustee.

OVERVIEW OF CIBC MELLON'S RISK MANAGEMENT PROGRAM

CIBC Mellon's Risk Management Program focuses on collaboration with peers and partnering with groups to support risk management excellence, risk awareness and risk-based decisions throughout the organization. The program implements risk coverage over all levels of the company through multiple lines of defence. The key components of the Risk Governance Program help us foster and reinforce a strong risk culture. These components include the Risk and Control Self-Assessment (RCSA), Key Risk Indicators (KRI), the Operational Risk Event report (ORE), and the evaluation of risk through the Operational Risk Committee's strategic review of the business units.

The program is continually assessed and enhanced to address emerging risks – such as geopolitical instability, digital innovation, cyber threats, third-party dependencies, and regulatory change – to support us in remaining proactive, vigilant and adaptive.

Three Lines of Defence

1

BUSINESS UNITS

(Designated Governance Officers)

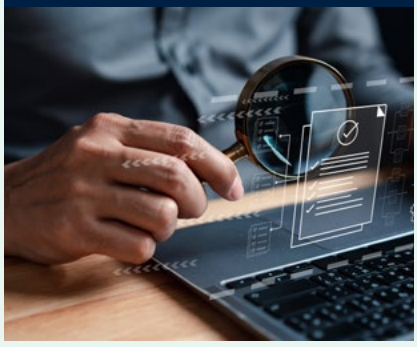
2

RISK MANAGEMENT AND GOVERNANCE PARTNERS

Risk Management and Compliance, Human Resources, Information Technology, Third-Party Governance, Finance, Legal, Business Continuity

3

INTERNAL AUDIT



FIRST LINE OF DEFENCE - BUSINESS UNITS

Our business units are the risk owners and are responsible for identifying, mitigating, monitoring and reporting all risks as appropriate. This includes maintaining a well-controlled environment that is monitored and proactively reassessed for appropriateness and completeness. It is updated or modified, as necessary, either to reflect changes in the business or to address emerging risks. The businesses are accountable for making risk management a fundamental responsibility in their line of business.

Every business unit at CIBC Mellon has a designated governance officer (DGO) who is a senior leader with a clear view into the operations of the business units they oversee. All employees are responsible for personally monitoring and reporting risk to their DGO. The DGO is also responsible for completing the annual Risk and Control Self-Assessment (RCSA). The RCSA is one of the key components of the Risk Management Program. It is a tool used by business units as an inventory and assessment of all business risks and the controls in place to mitigate each risk. The RCSA process is overseen by the Risk Management Department and Operational Control.

“In an organization, an effective governance program and a resilient risk culture go hand-in-hand. You cannot have one without the other. Our multiple lines of defence strengthen CIBC Mellon’s risk culture by embedding the core concept of personal responsibility across the organization.”

TIZIANA MANCINI

Vice President, Operational Risk

SECOND LINE OF DEFENCE - RISK MANAGEMENT AND GOVERNANCE PARTNERS

CIBC Mellon governance and oversight functions independently identify, measure, monitor, effectively challenge and report the first line of defence's identification, assessment and management of Operational Risk. Although primary risk oversight at CIBC Mellon is the responsibility of Risk Management and Corporate Compliance, all governance partners provide support, guidance and direction to business units on issues that require specialized knowledge and skills. Governance partners within CIBC Mellon include Legal, Finance, Information Technology, Human Resources, Third-Party Governance, Treasury Risk and Business Continuity Management. They provide input into new strategic initiatives of the various lines of business and set standards to promote consistency of approach in the management and the reporting of risks that fall under their area of expertise.

The Risk Management group, in conjunction with Operational Control, oversees the RCSA process. They review and challenge each RCSA concurred upon by the DGO, supporting that risks are properly managed across the company, within corporate guidelines and limits. The RCSA is a working document for each business unit, and is updated with regular reviews to include changes such as new business processes, product launches or updated regulations.

Operational Control provides an assessment on the controls used by the lines of business to mitigate its risks documented in the RCSA. Using a risk-based approach, with a focus on controls used in high risk processes, the control team develops its test plans. These plans can include reviewing both the design and operating effectiveness of the controls within the business. The group is also responsible for working with our internal and external auditors to produce the CIBC Mellon System and Organizational Controls (SOC1) Report. This report provides assurances regarding the strength of internal CIBC Mellon controls that may be relevant to clients' financial statements. The SOC1 Report is provided to clients and their auditors to affirm that our internal controls have the necessary design and operational effectiveness to achieve the controls' stated objectives.

Key Risk Indicators (KRIs) are measurements of quantitative data that help to detect risk issues and trends that are occurring in respective lines of business and may result in operational losses to the company if not appropriately acted upon. Lines of business must use these quantitative measurements to monitor the risks associated with achieving key performance objectives. Risk Management reviews and challenges the quality of the KRIs and oversees that any breaches experienced are being addressed appropriately.

Another key component in the Risk Management Program is the reporting of Operational Risk Events (ORE). Should an error occur, CIBC Mellon's business units are required to complete an ORE report – regardless of whether there is a financial impact, and irrespective of the size of the impact. This enables the capture of "near miss" scenarios. ORE reports are used to categorize operational errors, and are then analyzed for patterns and trends to identify and implement additional or new controls to reduce future errors. Any control deficiencies identified must be incorporated into the relevant RCSA, along with the action plan to address the deficiency.

OPERATIONAL RISK COMMITTEE (ORC)

CIBC Mellon's ORC includes representatives from the governance groups, Internal Audit as well as CIBC Mellon's Leadership Team. All business units present to this committee, providing information on their inherent risks, control strategies and emerging risks and trends. As the third key component of the Risk Governance Program, the formal review of operational risk through this committee supports the appropriate governance group oversight while ensuring business line management maintains accountability for identifying and managing the risks inherent in the products, services and activities for which they are responsible.

THIRD LINE OF DEFENCE - INTERNAL AUDIT

Risk Assurance includes the Internal Audit function, which reports to the Audit Committee of CIBC Mellon's Board of Directors. Internal Audit provides the committee, the Board and CIBC Mellon's senior management with independent and objective risk assurance and advisory services regarding the adequacy and effectiveness of CIBC Mellon's risk management, internal control and governance processes. Internal Audit uses a multi-faceted approach, which includes risk-based audits (including operational, technology, financial and regulatory audits), proactive and continuous monitoring of corporate-wide initiatives and the provision of value-added advisory services. The risk-based audit cycle is based on inherent and residual risk assessments. Audit results and the status of remediation of audit observations are reported to senior executives, both parent audit groups and quarterly to the Audit Committee of the Board.

"Our Internal Audit function continues to innovate through the adoption of new technologies and by embracing a mindset of continuous improvement. This is key to ensuring we remain effective in providing value and driving positive organizational change."

BEN KENTON

Chief Internal Auditor

OUR COMMITMENT TO PROTECTING OUR CLIENTS

CIBC Mellon's risk culture is strengthened by embedding the core concept of "risk management is every employee's responsibility." To this end, the purpose of CIBC Mellon's Risk Governance Program is to deliver value to clients by providing assurance that our risks are being appropriately identified, measured, managed and reported. By fostering a secure control environment and continuously reinforcing risk awareness across CIBC Mellon, we are not only protecting our company, employees and our reputation but also serving our clients' interests and the many stakeholders in Canada's capital markets who we work with every day.

A strong risk culture is required to support the risk appetite of the organization. Risk culture refers to the desired attitudes and behaviours relative to risk-taking. The main objective in establishing a risk culture is demonstrating behaviours in an organization that shape risk decisions of management and employees. A significant element of risk culture is a common understanding of an organization and its business purpose; understanding that risk and compliance requirements apply to everyone in working towards achieving business goals.

Culture risk is the risk that the values and beliefs guiding employees' behaviour and decision-making are adversely contrary to the company's vision, values, strategy and reputation.

CIBC MELLON'S RISK CULTURE HAS BEEN DESIGNED TO DEMONSTRATE OVERSIGHT AND GOVERNANCE BY:

1. **Defining threshold levels for measuring behaviours within CIBC Mellon**
2. **Ensuring appropriate indicators are in place to support the alignment between CIBC Mellon's vision and values, established processes and activities and behaviours of individuals and groups**
3. **Ensuring monitoring and reporting of culture risk indicators to the Leadership Team and the Boards of Directors**

The focus on risk appetite, supported by our risk culture has demonstrated we are successful in managing and measuring risk, with effective governance and controls that our clients would expect of us.

REGULATORY NOTICE - CULTURE RISK MANAGEMENT

The Office of the Superintendent of Financial Institutions (OSFI) published a regulatory notice setting out its expectations for managing culture risk under the key areas of governance, fostering desired culture and managing culture risks.

In its notice, OSFI defines culture risk as the "misalignment between a financial institution's stated desired culture and its actual culture that may prevent it from achieving its objectives." The regulator also provides preliminary considerations to guide the development and maintenance of the industry's culture risk management programs. The questions posed by OSFI elaborate on culture expectations as laid out in both OSFI's Culture Risk Management Regulatory Notice and its Corporate Governance Guideline.

MEASURING CULTURE RISK

At CIBC Mellon, our culture is shaped by both structural elements, such as our policies, processes, and procedures and human elements, including our shared beliefs, norms, and values. Together, these factors influence how we behave, make decisions and conduct business. Our culture is built on the underlying ideas and expectations that support our values and guide the way we work every day.

WE MEASURE CULTURE IN THE FOLLOWING WAYS:

Regular employee surveys which gather data on employee perceptions of various cultural aspects.

Key metrics and indicators: employee engagement, inclusion, turnover, absenteeism, internal movement/ promotion rates.

IMPLEMENTING STRONG THIRD-PARTY GOVERNANCE OVERSIGHT

A good third-party governance policy includes direction and guidance to help ensure that risks are identified and managed prudently, consistently, in compliance with laws and regulations. It should also addresses the key requirements in the selection, classification, performance measurement, purchasing standards, negotiation, and governance of vendors.

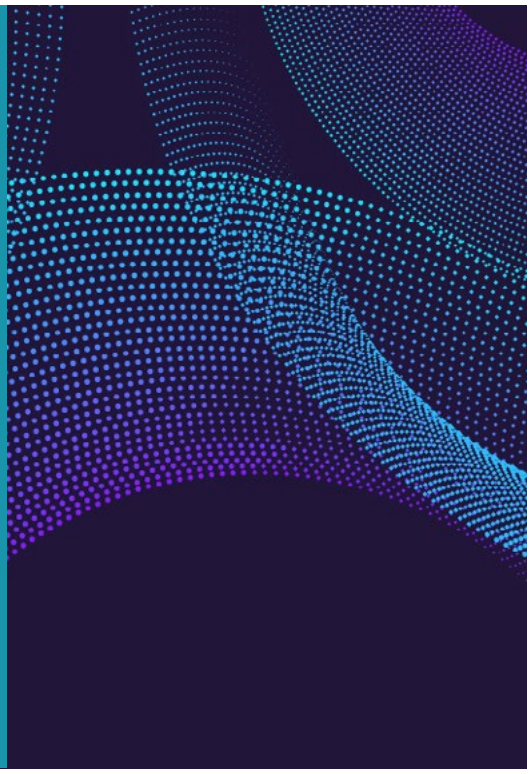
Agreements should hold vendors accountable to standards for performance with regular due diligence reviews and appropriate reporting requirements. For vendors whose services are deemed critical, including technology-related vendors, additional controls and monitoring are established to provide further assurance that additional risks related to the vendors, for example, business continuity, cybersecurity, and risks related to the supply chain, are being managed properly.

When responding to risks related to exposure services, such as artificial intelligence or cloud solutions to name a few, an integral step is to ensure service provider reviews are being conducted on a frequency commensurate with the risks associated with the service. While this is an important component of vendor selection and onboarding, it is imperative to continue to review vendors throughout the duration of the relationship. There are multiple ways vendors can provide assurance that clients' data is protected, for example by having multiple redundant data centres, comprehensive disaster recovery plans and by setting high standards for controls in place that address information security and data loss prevention.

CIBC MELLON'S APPROACH TO THIRD-PARTY GOVERNANCE

CIBC Mellon has an established Third-Party Governance Program through which it defines the requirements and frequency of oversight of our vendors. Through this program, we document and hold vendors accountable to standards for performance with regular due diligence reviews and appropriate reporting requirements. For vendor services defined as critical we implement additional controls and monitoring that provide further assurance that risks related to our vendors, the supply chain, and the services we receive, are being managed in accordance with CIBC Mellon's requirements – this is all part of our goal to carry out our client service and business operations with the highest standards for resiliency, governance and operational excellence.

As part of our global enterprise, we also work closely and collaboratively with our stakeholders, CIBC and BNY, to leverage their scale, governance and vendor relationships, when appropriate. A core element of our Third-Party Governance Program is overseeing the services our parents deliver to us, just as they exercise governance over the functions CIBC Mellon performs on their behalf.



KEY THEMES IN THIRD-PARTY GOVERNANCE AND OVERSIGHT

When it comes to managing due diligence processes with third-party relationships, today's market participants face heightened regulatory oversight requirements focused on, for example, subcontractor due diligence and sanctions and foreign interference screening. There are also growing expectations around technology enablement and innovation which are expected to further increase in complexity.

AI is rapidly transforming third-party services. To manage this class of outsourcing risk, CIBC Mellon has set contractual controls around the use of AI and a due diligence process that is part of our ongoing monitoring and risk mitigation practice. This applies for scenarios in which the use of AI already exists or is being contemplated. These established processes provide the opportunity to explore more extensively how AI is being used, establish guardrails and contemplate future use cases.

We know clients are looking for more than a third-party vendor, they want to find and build strategic relationships with trusted alliances: service providers that help to forecast opportunities, drive strategic plans and make it easier for clients to achieve their business goals.

CURRENT TRENDS IN INTERNAL AUDIT

CIBC Mellon is focused on a number of areas of key risk and regulatory change across the Canadian landscape as reflected in the updated OSFI guidelines: E-21, B-13, B-10, Integrity and Security, and the overall convergence of risks. These include:

Operational Risk and Resilience: There is a need for organizations to develop their risk management processes to focus on critical operations and the mapping of process dependencies. CIBC Mellon's Enterprise Risk Program incorporates this in addition to its core risk management and recovery processes.

Technology and Cyber Risk Management: Establishing and maintaining robust risk processes and compliance is key in the current environment of increased business transformation. Against the current backdrop of digitization, the adoption of new technologies, automation of manual processes and the implementation of AI solutions, it is critical to consider the increasing sophistication of cyber-related attacks against financial institutions.

Third-Party Risk Management: With the continued development of third-party relationships, we are seeing an increased need for focus on assessing various risks, including concentration risk, residual risk, exit strategies and the review of subcontractors.

CIBC Mellon's Internal Audit team's focus is aligned with these key risks along with others, including anti-money laundering (AML), Data Risk Management, Enterprise Architecture and Information Security. Internal Audit performs advisory reviews, management consultations, and advises on key developments, changes and areas of emerging risk. Our Audit Innovation Program is concentrated on being data- and risk-driven, with the adoption of enhanced technology, analytics and AI tools and the upskilling of our people.

WHAT COULD THE EVOLUTION OF INTERNAL AUDIT LOOK LIKE?

Internal Audit departments will continue to innovate to remain relevant in a transforming world, with proactive and forward-thinking approaches to the adoption and development of new technologies, including audit automation, data analytics and AI, being essential. With the nature and scope of audits evolving, alongside the emergence of new risks, audit teams must adapt to enhance an organization's ability to create, protect and sustain value.

CORPORATE COMPLIANCE IN TODAY'S REGULATORY ENVIRONMENT

Financial institutions are experiencing an increasing number of applicable regulatory requirements on a broad array of topics. It is critical that financial institutions be proactive in the continuous monitoring of their regulatory environment to allow for long lead times to understand the impact of emerging requirements and absorb the regulatory change. It is also important to periodically review controls using a risk-based approach to ensure they remain effective and continue to meet expectations in the evolving regulatory environment.

A key theme that continues to be an area of high inherent risk for Canadian financial institutions is anti-money laundering. AML regulatory requirements and expectations continue to increase and the impacts of not meeting regulatory expectations are becoming more significant. A financial institution must be nimble to adapt to this environment and ensure that their AML program remains appropriately resourced and controlled in a manner that is commensurate with the risk.

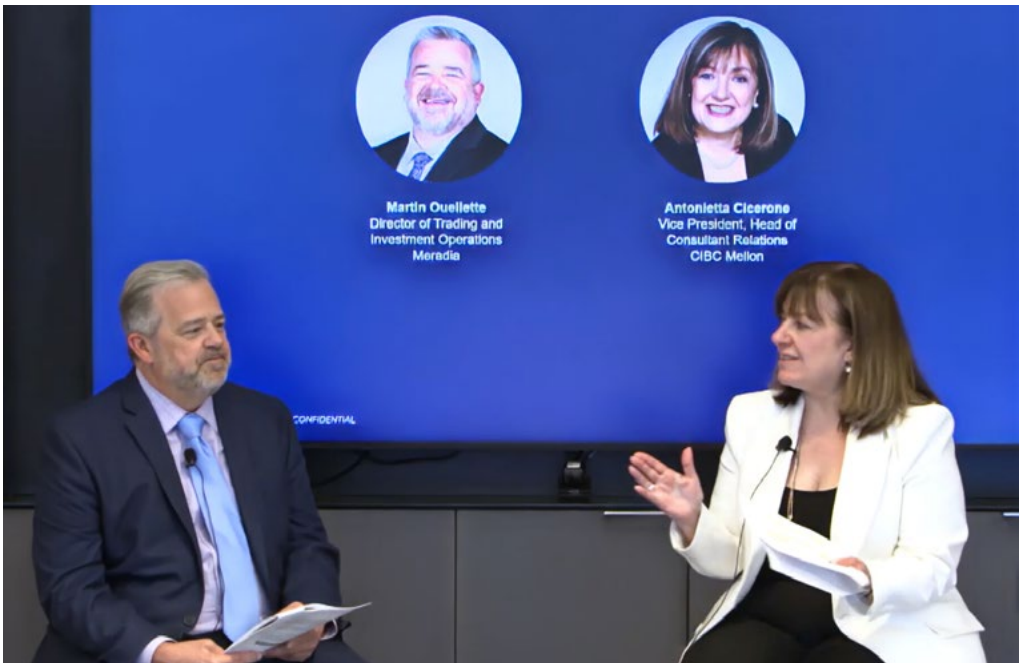
Foreign interference is a threat that is receiving attention from the Canadian government. Measures have been taken to expand OSFI's mandate to ensure that financial institutions protect themselves against threats to integrity and security, including foreign interference. OSFI considers this a key priority and has established a National Security Sector to focus on these threats. OSFI's Integrity and Security Guideline is now in force and measures are being taken to develop or enhance guidance to support this mandate.

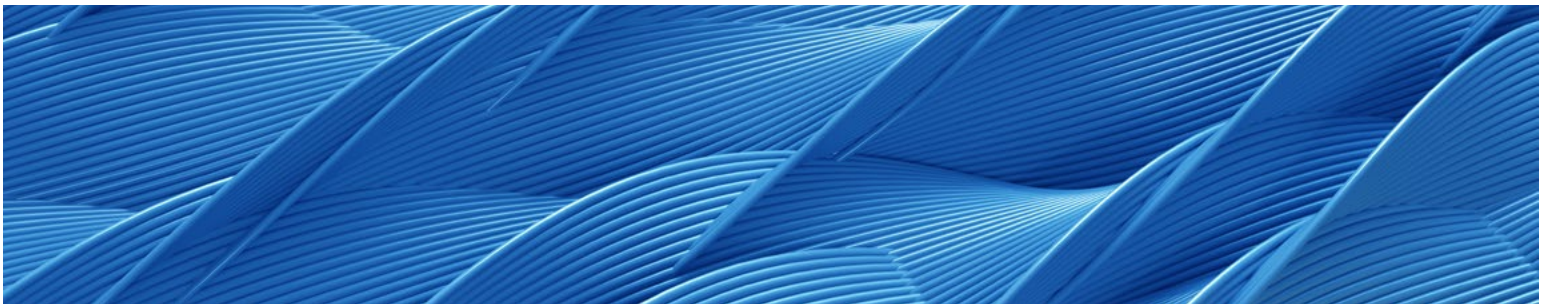
“As complexity and regulatory expectations increase, consultants act as strategic partners, supporting implementation, providing constructive challenge and strengthening governance frameworks.

Their role advances governance maturity by addressing key risks and reinforcing data integrity, leadership engagement and effective oversight foundations.”

ANTONIETTA CICERONE

Vice President, Head of Consultant Relations





THE EVOLUTION OF ORGANIZATIONAL RESILIENCY

Organizational resiliency programs continue to evolve in response to changing regulations, threats and risks. For instance, OSFI recently issued its E-21 guideline on operational resiliency where it details organizations' responsibility to understand the end-to-end requirements necessary to provide a critical service, either to end clients or to the financial services sector as a whole.

CIBC Mellon's Business Continuity Management (BCM) Program has a variety of planning and preparedness exercises to ensure that we maintain critical services at all times. Those exercises may be jointly carried out with our vendors by participating in their disaster recovery tests, which enables us to validate our respective recovery time objectives for supporting our Service Level Agreements in delivering services to our clients.

UPHOLDING THIRD-PARTY STANDARDS: ISO CERTIFICATION

In Business Continuity, adhering to third-party standards can help clients' businesses uncover opportunities for improvement, further enhance plans and certify preparedness to their leadership, their clients or prospects and other key industry stakeholders. An example of this is the British Standards Institution's ISO certification. Globally recognized, they help over 84,000 clients in 193 countries understand, assess and develop new standards to perform better in various situations. They offer a variety of certifications ranging from energy management requirements to occupational health and safety. CIBC Mellon maintains its ISO 22301 certification for business continuity. BSI Canada, as our external certification auditor, periodically reviews our programs, policies, procedures, and personnel and facilities to validate that they meet the ISO 22301 list of controls on an annual basis. Delivery of critical services is our key priority, and ensuring that we have a mature, robust, and ready BCM Program enables those critical services for our clients.

TECHNOLOGY AND RESILIENCY

Technology-related incidents impacting business operations are widely publicized in the media and continue to affect businesses across Canada and the globe at a greater frequency in today's highly-connected, digital world. Institutional investors, regulators and stakeholders across financial services and other industry segments are seeking assurance from their suppliers and partners that they have the processes in place to mitigate the effects of unexpected incidents, disruptions and threats on critical services.

CIBC Mellon has and will continue to take actions to sustain the high-quality service, stability and flexibility clients have come to expect of us. As a trusted safeguard of more than $3.3 trillion of assets held on behalf of banks, pension plans, investment funds, corporations and other institutional investors, we recognize the importance of our resilience to our clients. That's why we continuously work to further reinforce our strong governance and control environment. We know we need to react to unplanned challenges in a prompt, organized and effective manner to continue to provide our services and solutions to our clients.

KEY THEMES FOR CYBER RISK MANAGEMENT

Third-party risk assessments: Having the right level of controls, governance, and oversight over our key service providers to make sure cyber risks, security risks or continuity risks are understood and mitigated wherever possible.

Monitoring for malicious activity: Understanding the relationships between third- and fourth-parties and if there is a major security event with an external vendor, understanding the level of exposure and the planned response.

AI practices and threats: Setting guidelines and governance for the appropriate use of AI tools and technologies within the organization. Understanding that bad actors are using AI to craft new lures and methods for attacking organizations people and technology.

Mitigating insider threats: Understanding who within an organization could pose a threat, either maliciously or unknowingly to the organization, who has access to information, what are the sensitive roles and what are the controls that could be put around those individuals.

CIBC Mellon leverages its parent companies, CIBC and BNY, for its security operations for areas including its technology, operations support and access management. In addition to ISO 22301, CIBC Mellon also maintains its ISO 27001 information security certificate.

It is a good practice for industry participants to modernize internal manual processes to reduce the risk of fraud and cyber risks.

Two standards that may be relevant to your business continuity and information security efforts are:

ISO 22301
Business Continuity Management System

ISO 27001
Information Security Management System

KEY RISK THEMES FOR 2026 – MARKET SCAN

THE FOLLOWING IS A SUMMARY OF THE KEY RISKS CURRENTLY FACING CANADIAN FINANCIAL INSTITUTIONS.

1. **Geopolitical Risk:** Heightened geopolitical tensions and the current tariff war have increased economic uncertainly and led to volatile markets.

2. **Digital Innovation Risk:** The widespread use and rapid adoption of digital technologies that requires new skills and security protocols.

3. **Cyber Risk:** Cyber threats are more frequent and complex. Costs of an attack have increased and costs to put in place stronger controls have increased.

4. **Third-Party Risk:** A more complex third-party landscape as firms outsource more services requires strong oversight of critical providers.

5. **Regulatory Landscape:** An increasing number of regulatory guidelines and requirements that have led to higher compliance costs.

> “In an evolving regulatory environment with rapid technological advances coming to the surface of the financial industry, organizations are placing continued emphasis on ensuring they have a comprehensive and stable risk culture.”

KELLY HASTINGS
Chief Risk Officer

CIBC Mellon's Governance Summit took place June 4-5, 2025 in Toronto and virtually. Please contact your Client Manager if you would like to receive a copy of the event recordings.

FOR MORE INFORMATION

If you have any questions or to learn more about the governance and risk themes discussed, please reach out to your CIBC Mellon Client Manager.

CIBC MELLON

A BNY AND CIBC JOINT VENTURE COMPANY[SM]

www.cibcmellon.com

000 - KL64- 09 - 25