



Insider Risk Management in Canada

Results of the Cross-Sector Survey 2025-26 by Deloitte and the
Canadian Insider Risk Management Centre of Excellence

About this report

This report details the results of the latest insider risk management national survey conducted by Deloitte Canada and the Canadian Insider Risk Management Centre of Excellence (CInRM CoE). As part of this survey, data were collected from Canadian insider risk management professionals regarding their perception of insider threats, as well as the control measures implemented within their organizations.

The data in this report are based on a survey conducted between April 2025 and June 2026. The survey was completed by senior executives from the security, fraud prevention, cybersecurity, information technology and human resources sectors. Respondents were drawn from a representative sample of Canadian industries, including subsidiaries of foreign companies, public-sector organizations, non-profit organizations and other private enterprises.

Unless otherwise indicated, all numerical data refer to the survey response results. The 2026 survey included a substantially larger and more diverse sample of Canadian organizations than the inaugural 2025 survey. While direct year-over-year comparisons should be interpreted with caution, broad trends continue to provide useful directional insight into the evolution of insider risk management practices across Canada. Accordingly, year-over-year comparisons are presented as directional rather than as statistically validated changes in the Canadian population. Greater emphasis is placed on the relative ranking of capabilities, recurring themes, and persistent areas of strength or opportunity. These results are anonymous, and only aggregated responses are reported.

Thank you to all survey participants for your continued support in this effort.

Foreword



**Pierre-Luc
Pomerleau,**
Ph.D.
Deloitte Canada
Partner,
Financial Crime



Victor Munro,
Ph.D.
Canadian Insider Risk
Management Centre of
Excellence
CEO, CInRM CoE

The conversation surrounding insider risk management has changed significantly over the past year. What was once viewed by many organizations as an emerging security concern is now recognized as a business imperative. Insider risk is no longer solely a cybersecurity issue; it is a strategic challenge that affects people, information, critical operations, reputation, and trust at the heart of every organization.

The findings in this second annual report show that Canadian organizations are making meaningful progress. More organizations are establishing governance frameworks, formalizing policies, deploying monitoring capabilities, and embracing a broader understanding of insider risk. Yet progress remains uneven. Many organizations continue to rely on reactive measures, leaving them exposed to risks that are increasingly detectable, preventable, and costly when left unaddressed.

This report arrives at a pivotal moment for Canada. Regulatory expectations are rising, zero trust principles are becoming mainstream, and artificial intelligence (AI) is fundamentally reshaping how employees access, share, and interact with information. At the same time, intellectual property theft, fraud, workplace misconduct, cyber sabotage, and activity from state-sponsored threat actors continue to reinforce a fundamental reality: trusted access remains one of the most difficult risks for organizations to manage.

The question facing leaders is no longer whether insider risk deserves attention, but whether organizations are prepared to manage it effectively. As budgets come under greater scrutiny, insider risk programs must demonstrate measurable business value, not only by preventing incidents, but by strengthening governance, protecting reputation, reducing operational friction, and enabling organizations to innovate securely and confidently.

Foreword

Since publishing our inaugural report, Deloitte Canada and the Canadian Insider Risk Management Centre of Excellence have had the privilege of working alongside organizations across critical infrastructure, financial services, government and higher education to help establish and mature insider risk programs. Those engagements, combined with our continued research and collaboration with international partners, reinforce an important lesson: while technology continues to evolve rapidly, successful insider risk management remains fundamentally about people, governance, and informed decision-making.

This year's report builds upon the foundation established in our inaugural publication while offering updated benchmarking data, practical observations from those in the industry at large, and actionable recommendations for organizations seeking to mature their capabilities. Whether your organization is establishing an insider risk program for the first time or refining an existing capability, we hope these findings provide valuable insight into where the Canadian marketplace is today—and where it must continue to evolve.

Ultimately, insider risk management is no longer simply about preventing the next incident. It is about enabling organizations to operate with greater confidence, resilience, and trust in an increasingly interconnected world. We hope this report continues to serve as both a national benchmark and a practical guide for leaders committed to building resilient organizations capable of managing the risks—and opportunities—that come with their most valuable asset: their people.

Pierre-Luc Pomerleau, Ph.D.

Partner, Deloitte Canada

Industry Advisory Council, Insider Risk Practitioner Alliance

Victor Munro, Ph.D.

Chief Executive Officer, Canadian Insider Risk Management Centre of Excellence

Secretary General, Insider Risk Practitioner Alliance

Table of Contents

Executive Summary	6-7
Introduction	8
Evolution of the Insider Threat	9-10
Insider Threat Management Capability	11-14
Sector Comparison	15
Conclusion	16
Key Contacts	17

Executive Summary

The 2025-2026 cross-sector survey results demonstrate that insider threat remains a significant risk for Canadian organizations, with nearly **three quarters of respondents reporting at least one incident over the past 12 months**. Despite a modest increase in awareness and in certain detection capabilities, overall program maturity remains uneven. Organizations continue to favour well-established traditional controls, such as pre-employment screening and access management, while more advanced capabilities in governance, continuous monitoring, and behavioural analytics struggle to take shape. The results also reveal significant disparities across sectors; the financial sector displays the highest maturity, while government and energy sector organizations face distinct challenges in governance, detection, and risk prioritization.



The results highlight a **critical need to accelerate program formalization and strengthen coordination across functions** to ensure proactive and effective management of insider threats.

01

Insider threats remain pervasive and incident volumes are rising

Nearly 73% of organizations reported at least one insider threat incident in the past 12 months. Affected organizations are reporting more incidents than before, indicating either an intensification of risk or improved detection capabilities¹. Negligence remains the most commonly reported insider threat, while workplace harassment and violence are emerging as the fastest-growing incident category.

02

Insider threat governance remains a main weakness

Program formalization continues to represent the greatest challenge. The proportion of organizations with a dedicated working group is 51%, while only 5% report having robust policies and frameworks in 2026. These findings reveal a persistent gap in integrated governance and cross-functional coordination.

1. Caveat : The absence or low number of reported incidents in certain sectors may reflect limited detection or reporting capabilities, rather than reduced exposure to insider risks.

Executive Summary

03

Traditional controls remain the most mature; however, more can be done on employee lifecycle assurance

Pre-employment background checks remain widely adopted (89%). Routine verification controls (57%), and formalized offboarding procedures (70%), signal that certain key control mechanisms across the employee lifecycle still require additional focus and maturation.

04

Advanced detection capabilities remain far from an optimum target state

Adoption of user and entity behavioural analytics (UEBA) capabilities is advancing, with the proportion of organizations that have reached at least an operational level of maturity being at 50%. Continuous monitoring, training, awareness, and incident triage capabilities remain limited in maturity across most organizations.

05

Maturity varies widely across sectors

The financial sector shows the highest level of maturity (3,67/5) but also remains the most exposed to insider threat incidents. Government organizations show lower maturity in governance and formalization, while the energy sector appears to be underreported on insider threat incidents despite elevated risks, particularly those related to IT sabotage and incidents of harassment or violence.

Canadian organizations continue to advance their management of insider risks, but the maturity of programs remains constrained by insufficiently structured governance, limited continuous monitoring, and low adoption of advanced prevention capabilities.



Insider risk maturity must be considered within a continuously evolving threat environment. As insider threats, technologies, and business operating models continue to change, organizations that do not periodically reassess their risks, benchmark their programs, and adapt their controls may experience a decline in relative maturity over time despite maintaining existing capabilities. Any extrapolation between industry sectors should be undertaken with caution.

Introduction

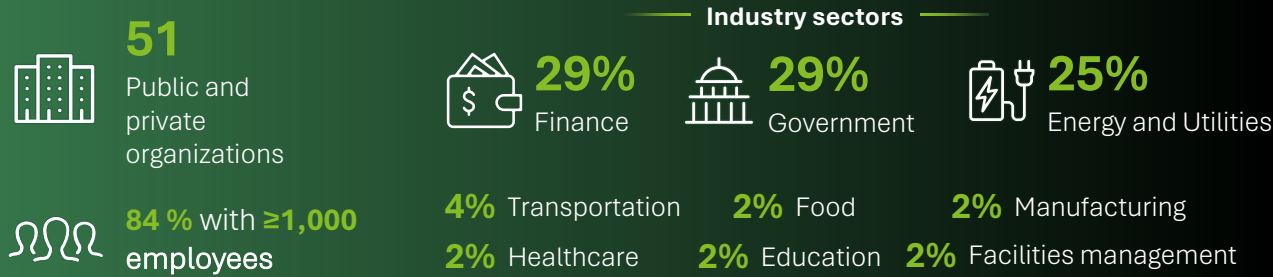
The insider threat landscape in Canada continues to evolve rapidly. Against a backdrop of digital transformation, hybrid work and the expansion of data ecosystems, organizations across the public and private sectors face growing insider risks, whether malicious or unintentional.

The 2026 edition of the Deloitte survey builds on the study conducted in 2025, enabling us to measure how the practices and maturity of Canadian organizations in insider risk management have evolved.

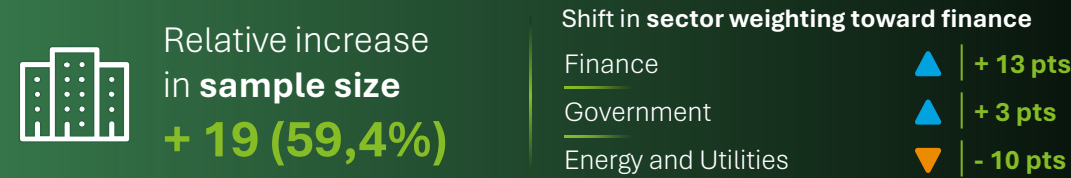
With legitimate access and an in-depth knowledge of systems, insider threat actors present a particularly complex risk profile, prompting organizations to rethink their approaches to trust, monitoring and accountability. In the face of increasingly sophisticated threats, organizations must continue to advance more mature insider risk management programs, incorporating greater cross-functional collaboration, heightened organizational awareness and a capacity for continuous adaptation.

Based on a methodology aligned with prior work, this second edition aims to provide comparative insight and to identify emerging trends to support organizations in strengthening their capabilities.

2026 Profile of participating organizations



2025 Compared to first edition of the survey

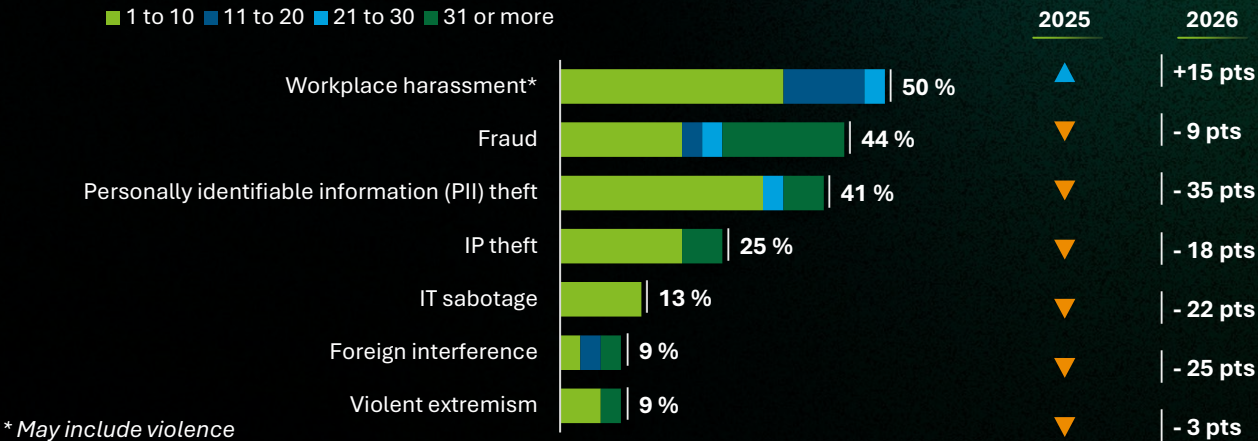


The results highlight several trends; however, they should be interpreted in the context of a larger sample size, changes in industry representation, and the fact that maturity levels are based on respondents’ self-assessments of their organizations’ capabilities. As a result, observed differences in maturity may reflect both changes in the composition of survey participants and differences in how organizations perceive and evaluate their own capabilities. Any extrapolation between industry sectors should be undertaken with caution.

Evolution of Insider Threat

Incident types and prevalence

Proportion of organizations experiencing ≥ 1 incident



Workplace harassment stands out clearly in 2026. This signal indicates that the risk profile is driven by sector composition², evolving reporting practices or greater visibility into workplace incidents.

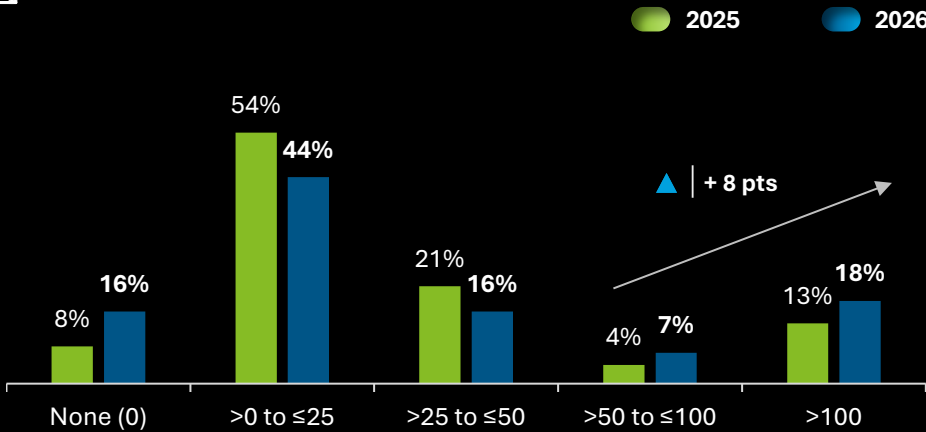


73% of organizations³ experienced at least one insider threat incident in the past 12 months.



60 % detected 25 or fewer insider threat incidents

25% report more than 50 incidents, an increase of 8 percentage points



Nearly three in four organizations report at least one insider threat incident, confirming the persistent scale of the risk.

2. This increase reflects a broader trend observed across Canadian government entities, where reported cases of workplace harassment and violence rose by 13% in 2023, reaching 2 129 cases in the federal public service. [Daniel Leblanc, CBC News, 2 mars 2026.](#)

3. Note: Results are based on 51 respondents; 12% declined to answer this question or did not provide a response.

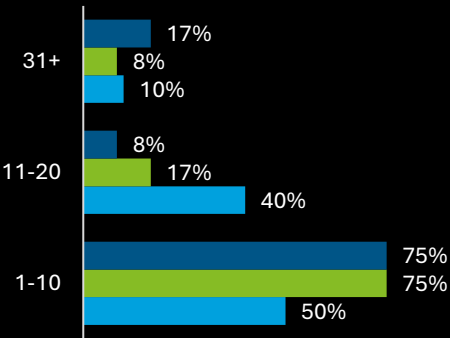
Evolution of the Insider Threat

Underlying intent types and prevalence

Among organizations that track insider threat incidents by underlying intent



Distribution of detected Incidents by underlying intent

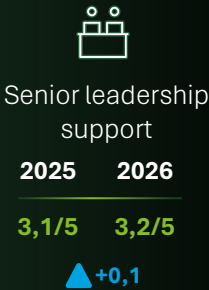
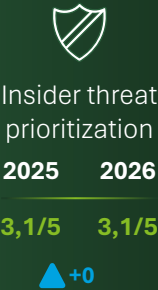
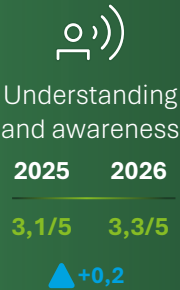


35% of organizations do not formally track insider threat incidents by underlying intent.

In 2026, insider threats remain a multifaceted challenge: **negligence is most common**, but malicious activity is nearly as widespread, underscoring the **persistence of intentional insider risk**.

Reported incidents remain **primarily concentrated in the 1 to 10 incident range**, regardless of intent. A meaningful share of **accidental incidents** are nonetheless reported in higher volumes.

Organizational engagement



The focus of organizations remained consistent across the past two years. Integrating insider threat into risk management and security **strategies still requires strong executive commitment** as well as greater organizational **prioritization** to deliver lasting gains.

“ We have an established IR Working Group that is in the process of developing a program framework and response protocols. **We are still pressing to get an executive-level steering committee that has proven to be difficult in getting traction/buy-in.** The IRWG has come a long way in establishing a collective recognition of the value of a viable Insider Risk Program. ”

Respondent from the Energy and Utilities industry

Insider Threat Management Capability Maturity

Capability maturity by sector

Capabilities	Financial	Government	Energy	Other*
Cross-functional working group	3,50	2,56	2,45	2,80
Insider threat framework and policies	3,63	2,78	2,50	2,75
Pre-employment background checks	4,50	4,44	4,27	4,00
Continuous or periodic background checks	3,00	3,78	2,70	2,40
Training and awareness	3,13	2,67	3,30	3,20
Formalized offboarding procedure	3,86	3,33	4,00	3,00
Incident triage and escalation process	3,38	2,78	3,40	3,75
Physical access controls	4,13	4,13	4,00	4,80
Logical access controls	4,25	4,38	4,64	5,00
UEBA	3,38	2,57	3,44	2,50
Average score by sector	3,67	3,34	3,47	3,42

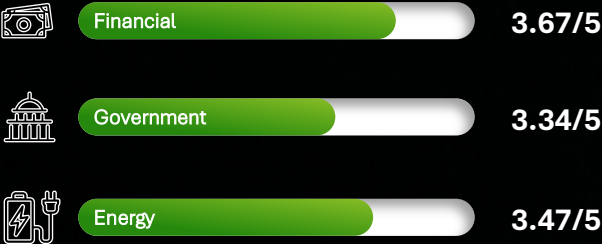
* Other industries are: Transportation, Food, Healthcare, Education, Manufacturing, Facilities Management

Maturity continuum legend

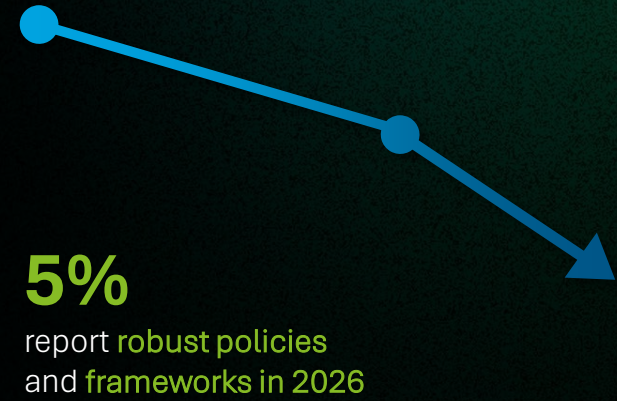
-  1 = Does not exist / Not planned
-  2 = Planned or in development
-  3 = Initial capability / Ad hoc
-  4 = Basic capability / improvement desired
-  5 = Robust capability / target state

Insider Threat Management Capability Maturity

Sector maturity gaps



Gaps in robust policies and frameworks



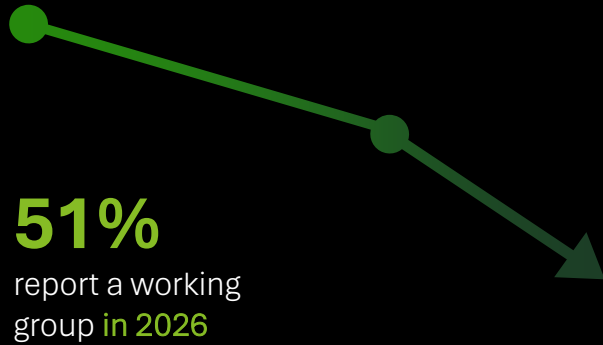
The financial sector stands out with the highest level of maturity in the area of insider risk management. Conversely, government and energy & utilities entities show a relative limited maturity, demonstrating less progress towards advanced capabilities.

38% of organizations have no formal policy or framework, indicating that several programs remain less defined in the prevention, detection and management of insider risks.



Insider risk governance remains largely informal

Gaps in dedicated working groups



The cross-functional working group remains one of the least mature elements of the insider threat management framework, illustrating a persistent gap in integrated governance and cross-functional coordination.

Training, awareness, escalation and triage still lack maturity

Escalation and triage process



43% reach at least basic capability...



...but only 8% have robust capability

Training/awareness programs



35% reach at least basic capability...



...but only 11% have robust capability

Insider Threat Management Capability Maturity

Several foundational controls display lower levels of maturity

Pre-employment background checks



86%
performed pre-employment background checks



89%
performed pre-employment background checks



Pre-employment **background checks** remain firmly well established across all sectors, and demonstrate **widespread adoption**.

Continuous background checks



62%
performed continuous background checks



57%
performed continuous background checks



Continuous background checks or assurance remain **less systematic**, with the exception of government organizations*, which display a higher level of maturity in this area.

Formalized offboarding procedure



81%
had procedures in place to manage the risks associated with departing employees



70%
had procedures in place to manage the risks associated with departing employees



The reporting indicates that organizations have not fully standardized the formalization of offboarding procedures **for departing employees**.

**This may be due to the adapted TBS Directive on Security Screening which was effective January 6, 2025, requiring federal government entities to conduct continuous assurance based on a risk assessment framework.*

Insider Threat Management Capability Maturity

Access controls remain among the most mature foundational capability



Physical and logical access controls **remain among the most** developed capabilities in the industry at large.

UEBA adoption seems to be increasing



However, UEBA remains **one of the least mature capabilities**: its adoption is driven by **sector risk exposure** rather than by organization size and organizations seeking to better contextualize individual-level risk behaviours, making it a **still-underused lever** for shifting from a reactive to a proactive posture.

From prevention to detection



Prevention
Access controls
Preventive posture



Detection
Behavioural monitoring
Proactive posture

Organizations have made greater progress in **controlling privileged access** than in **continuous monitoring of pre-defined high-risk behaviours**, highlighting a remaining gap between prevention and detection capabilities.

Sector Comparison

Financial

Industry maturity leader... but more exposed to insider risks



3.7/5

Highest average maturity score for insider risk management

87%

experiencing ≥ 1 incident in the past 12 months (the highest)

Strategic Priority



Strengthen continuous screening and employee awareness programs



54%

of financial sector organizations that reported at least one insider threat incident experienced fraud, making it the most prevalent threat in the sector.

Government

Strong controls, but governance and proactive capabilities lag industry peers



2.8/5

Average maturity score for formalization of policies and frameworks

2.6/5

Average maturity score for the cross-functional working group

Strategic Priority



Strengthen governance and awareness



18%

Foreign interference and violent extremism incidents are reported almost exclusively by government entities (18% of organizations respectively).



63%

Nearly one third of organizations that reported workplace violence and harassment incidents come respectively from the Government and Energy sectors (31% each).

Energy and utilities

High incident exposure despite lower executive prioritization



2.8/5

Average executive prioritization score for insider threat (the lowest in sectoral comparisons)

46%

experiencing ≥ 1 incident in the past 12 months (the highest in sectoral comparisons)

Strategic Priority



Invest in awareness and detection



75%

Reporting on IT sabotage incidents is concentrated in the Energy and Utilities sector, representing 75% of organizations that experienced this type of incident.

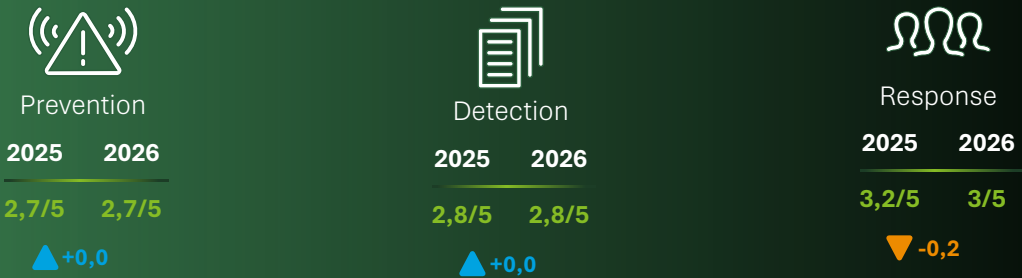
Conclusion

Proactive Posture



Modernizing detection tools must not come at the expense of foundational controls. As the adoption of advanced capabilities increases, several proven controls to manage risk across the employee life cycle are eroding. This imbalance risks having organizations build sophisticated capabilities while not maintaining pace on foundational controls which are weakening due to the evolving insider threat environment—particularly at sensitive transitions: access, mobility and offboarding.

Capability maturity diagnostic



Canadian organizations have crossed the recognition threshold: insider threat is now being measured as an **enterprise risk**. This awareness, however, has yet to translate into structured programs – **barely 5% have robust policies and frameworks in place** - leaving a significant gap between intention and execution.



The general industry risk profile is varied; **workplace harassment and violence figures** demonstrate a need for further consideration in organizations’ risk mitigation strategies. Combined with the persistent predominance of negligence-related incidents, this calls for **refocusing programs on the human factor as much as on maintaining and evolving technical controls**.



The next milestone is proactivity. No sector reaches the 3/5 threshold for a proactive posture. Advancing overall maturity in this area over the next year will require integrated governance, the refining of continuous monitoring processes based on a defined risk framework, and strengthened cross-functional coordination.

Key Contacts



Pierre-Luc Pomerleau Ph.D.

Partner, Financial Crime

E : ppomerleau@deloitte.ca



Victor Munro, Ph.D.

Director, Financial Crime

E : vmunro@deloitte.ca

Executive Director, CInRM CoE

E : victor.munro@cinrmcoe-cdecgrinc.ca

Contributors



Isabelle Fraser
Manager



Mélissa Bourgie
Manager



Sébastien Bodart
Analyst



**Sabrina Marleny
Cruz Jimenez**
Analyst

About Deloitte Canada

At Deloitte, our Purpose is to make an impact that matters. We exist to inspire and help our people, organizations, communities, and countries to thrive. Our work underpins a prosperous society where people can find meaning and opportunity. It builds consumer and business confidence, empowers organizations to find imaginative ways of deploying capital, enables fair, trusted, and functioning social and economic institutions, and allows our friends, families, and communities to enjoy the quality of life that comes with a sustainable future. And as the largest Canadian-owned and operated professional services firm in our country, we are proud to work alongside our clients to make a positive impact for all Canadians.

Deloitte provides industry-leading consulting, audit and assurance, tax, advisory and managed services to nearly 90% of the Fortune Global 500® and thousands of private companies. We bring together world-class capabilities, insights, and services to address clients' most complex business challenges.

Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

To learn more about Deloitte Canada, please connect with us on [LinkedIn](#), [X](#), [Instagram](#), or [Facebook](#).

© 2026 Deloitte LLP and affiliated entities.

About the Canadian Insider Risk Management Centre of Excellence (CInRM CoE)

Founded in 2022, the Canadian Insider Risk Management Centre of Excellence (CInRM CoE) is federally incorporated under the Canada Not-for-Profit Corporations Act, as a public service body, not-for-profit entity and soliciting corporation, based at Carleton University, Norman Paterson School of International Affairs (NPSIA).

The CInRM CoE promotes academic, private, and public partnerships to generate academic research, provides training and learning opportunities, promotes knowledge sharing, and augments resources and capabilities in the professional market to mitigate insider threats to Canadian organizations and critical infrastructure. The scope of its services is offered to all Canadian federal, provincial, territorial (FPT) and Indigenous organizations—with a particular focus on fostering critical infrastructure (CI) resiliency—subject to resourcing.

The CInRM CoE fosters an interdisciplinary approach to insider risk management towards the promotion of industry best practices and innovation within an evolving threat environment. Funded by industry contributions and research grants, we offer a national and centralized capability on all matters related to insider risk management. Our products and services include research and analysis, facilitating workshops and knowledge sharing events with subject matter experts, generating lessons learned, providing workplace training, and advocating for new initiatives to enhance Canada's collective resiliency against insider threats. This work is established on a foundation of information sharing among a trusted community of security, intelligence, and defence professionals.

© 2026 Canadian Insider Risk Management Centre of Excellence