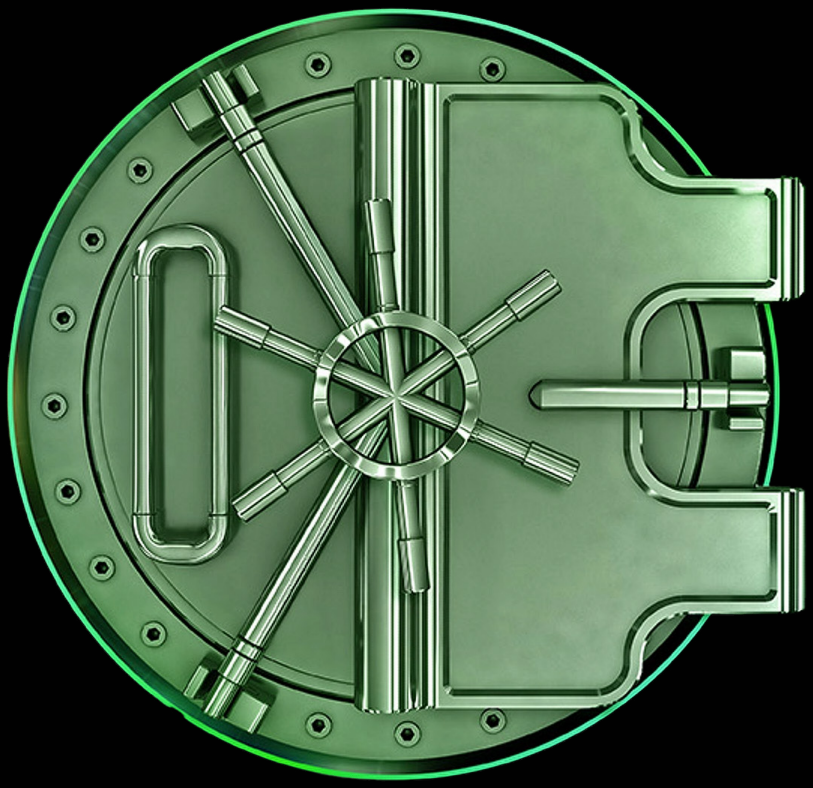
Deloitte.

CANADIAN INSIDER RISK MANAGEMENT CENTRE OF EXCELLENCE
CENTRE D'EXCELLENCE CANADIEN POUR LA GESTION DES RISQUES INTERNES



Insider risk management in Canada

Findings from Deloitte and the Canadian Insider Risk Management Centre of Excellence's 2024-25 cross-industry survey

September 2025

About this report

This report details the findings from Deloitte Canada and the Canadian Insider Risk Management Centre of Excellence's (CInRM CoE) inaugural Insider Risk Management industry survey. Through this survey, data was collected from Canadian insider risk management practitioners on their perceptions of insider threats and their organizations' associated controls.

The data in this report is informed by a survey conducted between September 2024 and April 2025. The survey was completed by senior leaders in security, fraud, cybersecurity, IT, and human resources from a cross section of Canadian industries, including Canadian subsidiaries of foreign companies, public sector organizations, not-for-profit organizations and other privately held companies.

The data in this report is complemented by interviews with leaders across Canada and insights from Deloitte's own subject matter experts, with experience both in Canada and globally. Quotations included in this report have been edited for readability.

Unless otherwise stated, all numerical data refers to the results from survey responses. These results are anonymous, with only aggregate responses reported.

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

Foreword

Pierre Luc Pomerleau, Ph.D.
Partner
Deloitte Canada

Victor Munro
Senior Manager
Deloitte Canada
Executive Director
Canadian Insider Risk Management Centre of Excellence

In an era marked by increasingly complex risk environments, insider threat remains one of the most difficult issues to manage across different categories of enterprise risk. This first-of-its-kind publication inspired by Deloitte Australia—the result of a collaboration between Deloitte Canada and the Canadian Insider Risk Management Centre of Excellence—offers a uniquely Canadian perspective on how organizations across sectors are perceiving and addressing this challenge.

Based on survey responses from senior professionals in security, cybersecurity, IT, fraud, and human resources, this report sheds light on how insider risk is evolving, how Canadian organizations are responding, and where there remain gaps in strategy, controls, and awareness. Complemented by interviews and expert insights, the report also explores real-world considerations and approaches that extend beyond theory.

What emerges from the data is clear: managing insider risk is no longer a peripheral issue—it is central to safeguarding organizational resilience, trust, and integrity. Yet despite increasing recognition of the threat, many organizations still struggle to quantify progress or justify investment. This is largely due to the intangible nature of prevention and being proactive, the difficulty in confirming past insider threat events, and the long-term horizon scanning required to realize the full benefits of a comprehensive program.

As the Canadian regulatory landscape evolves—driven by guidance form Public Safety Canada, the Canadian Centre for Cybersecurity, and the Office of the Superintendent of Financial Institutions—organizations must shift from reactive measures to proactive, enterprise-wide strategies. This report serves not only as a benchmark for industry maturity, but as a Made-In-Canada roadmap to strengthen a proactive posture, foster cross-functional collaboration, and embed insider risk management as a core organizational discipline.

We hope this inaugural edition will stimulate critical dialogue at all levels of the enterprise, including the C-Suite, and support organizations in building the programs needed to meet the insider risks of today—and tomorrow.

Over the last 22 years, I've worked at the intersection of national security, public safety, and enterprise risk—first as a Canadian federal public servant for 18 years, and more recently as a senior advisor in the private sector. For the past seven years, my doctoral research has focused on insider threat monitoring and detection, allowing me to observe first-hand the evolution of organizational capabilities and mindsets across sectors and domains.

One of the clearest lessons from this journey is that insider threats transcend boundaries. They cannot be addressed by any single corporate vertical—be it security, cyber, fraud, or compliance—alone. Insider risk demands a holistic, integrated approach, one that embeds trust, accountability, and visibility into the everyday fabric of organizational life.

This report, built on the insights of practitioners from across Canada, highlights just how far we've come as an industry—and how far we still need to go. The most mature programs we observed in our survey shared several key traits:

- Robust cross-function coordination,
- A commitment to accelerated policy development and implementation,
- Continuous monitoring using User and Entity Behaviour Analytics (UEBA), and
- An understanding of how organizational culture and employee behaviour shape both risk and opportunity.

We also found that many Canadian organizations are now at an inflection point—poised to elevate insider risk management from a siloed activity to an enterprise-wide priority. This report provides a critical tool to help move those conversations forward with the C-Suite. Whether launching a dedicated program or looking to mature an existing one, the insights here can help bridge the gap between awareness and action.

This is a pivotal time for insider risk management in Canada. I am proud to present this report as both a national benchmark and practical guide for leaders committed to building more resilient organizations.

Contents

Executive Summary

This 2024-25 cross-industry survey reveals that while Canadian organizations generally demonstrate a moderate understanding of insider risk, it remains underestimated relative to other enterprise threats. Despite growing recognition, most insider risk programs lack sufficient executive-level support to drive proactive, enterprise-wide action. The continued visibility of insider threats has been sustained by emerging regulatory guidance, adoption of industry best practices, and ongoing high profile incidents across sectors.

Deloitte's anonymous survey of Canadian practitioners helps to provide insights on how organizations may address insider risk. In providing this benchmark four key insights have emerged.

1

Canadian organizations have to strengthen cross-functional coordination

It is necessary to strengthen internal risk management governance by creating dedicated working groups and cross-functional committees involving human resources, IT, ethics and compliance, security, legal, business operations, and finance.

2

Policy development and implementation must be accelerated

Insider risk management policies need to be developed and implemented more quickly. Clear guidelines on how to detect, address, and respond to insider threats are needed to strengthen commitment across the organization.

3

Ensure continuous monitoring and integrate tools such as UEBA

The lack of ongoing monitoring after hiring, with few routine employee ongoing screening, exposes organizations to undetected risks. It is crucial to integrate tools such as user and entity behavioural analysis (UEBA) to identify risky behaviour throughout the employee lifecycle.

4

Do not neglect behaviours outside digital systems

Insider threats often result from complex psychological and behavioural factors that do not manifest themselves solely on virtual platforms. Analysis of non-digital behaviours, such as in-person interactions and changes in employee habits, must also be a priority in holistic insider risk management.

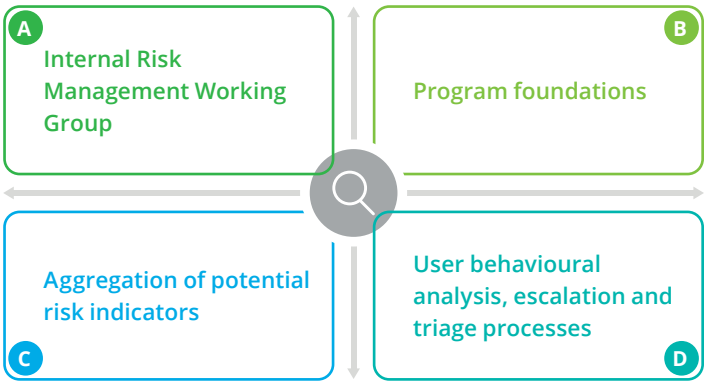
Introduction

The insider threat landscape in Canada is evolving rapidly. As organizations across public and private sectors navigate a heightened risk environment marked by digital transformation, hybrid work, and expanding data ecosystems, the threat from within—whether malicious or unintentional—has become increasingly difficult to detect and mitigate. While traditional security programs have focused on external adversaries, institutions are now beginning to reckon with the reality that insider threats, with their authorized access and contextual knowledge, present a more complex and persistent risk. This shift demands not only new technologies, but new ways of thinking about trust, monitoring, and organizational accountability.

Canada is no stranger to the consequences of insider threat attacks. Over the past decade and a half, several high-profile breaches—ranging from unauthorized disclosures of sensitive government information to trusted employees exploiting system access for personal or criminal gain—have highlighted the urgent need for resilience. These events serve as stark reminders that insider risk is not theoretical; it is real, and it carries profound operational, reputational, and legal implications. As threats become more sophisticated and the cost of inaction grows, Canadian organizations must take deliberate steps to build mature insider risk programs rooted in cross-functional collaboration, cultural awareness, and continuous adaptation.

Deloitte's 2024-25 Insider Risk Management Survey

The purpose of this study was to assess the current state of insider risk management practices in Canadian organizations. The research team conducted a replication study of research done by Deloitte Australia in 2023, and asked survey participants to answer 34 questions, that could be further consolidated to 10 main questions, focusing on four control areas of control, aligned with the following framework:



Insider threat refers to the unintended or malicious exploitation of privileged access to assets that are sensitive and critical to an organization's mission, including its personnel, resulting in adverse consequences.

About the participating organizations

32

Participating private and public organizations

- **39%** of organizations had fewer than 10,000 employees
- **26%** of organizations had fewer than 1,000 employees

7

Industries represented

- Aerospace and Defence, Energy and Utilities, Facilities Management, Finance, Food, Government, Manufacturing sectors

Qualitative and Quantitative

Information captured

- Quotations included in this report are presented anonymously and have been edited for readability
- Unless otherwise stated, all numerical data refer to the results from the survey responses

Survey participants were asked to estimate the total number of insider threats experienced by their organization over the past 12 months.

Let's start with a striking statistic: 73% of participating organizations experienced at least one internal threat incident in the past year. This shows how insider threats are a pervasive and worrying reality for businesses in both the public and private sectors in Canada.

Canadian organizations rate their level of awareness of insider threats, the priority given to these risks, and the executive support they receive to address them at an average of 3.1 out of 5. While the score reflects some degree of recognition of internal threats, it also shows that there is still work to be done to fully integrate these issues into organizations' overall strategy.

73%

Of participants have experienced an insider incident in the last 12 months

3.1/5

Overall awareness and understanding rating

3.1/5

Rating for insider threat as a priority

3.1/5

Rating for executive level support for insider threat

Defining and tracking insider threats: Types vs. Outcomes

Organizations should implement comprehensive tracking of all three primary categories of insider threat—accidental, negligent and malicious—because each represents a distinct pathway to potentially severe harm, often with overlapping consequences. Accidental and negligent acts, such as misdirected emails or failure to follow established security protocols, can still lead to outcomes like data exfiltration or operational disruption, even if they are not driven by the same underlying motivations that are more commonly associated with malicious insider threats.

Without systematic monitoring and analysis, these activities often go undetected until the damage is irreversible. Comprehensive tracking allows organizations to identify behavioural and technical indicators early, correlate incidents across business units, and measure trends over time—thereby enabling targeted interventions, strengthening controls, and reducing the risk of cascading impacts that could undermine both security and trust.

Types

Accidental

Unintentional actions by an employee that result in harm or increased risk to the organization, often due to human error, lack of awareness, or misjudgment. Examples include sending sensitive information to the wrong recipient or misconfiguring a system without realizing the security implications.

Negligence

A failure by an employee to follow established policies, procedures, or security protocols, despite having the knowledge or training to do so. Negligent acts are preventable and stem from disregard, carelessness, or failure to exercise due diligence, such as ignoring mandatory security updates or bypassing access controls.

Malicious

Intentional actions by an employee aimed at causing harm or achieving personal gain, driven by motives such as financial benefit, revenge, ideology, coercion, or loyalty to an external entity.

This category includes activities like data theft, fraud, sabotage, workplace violence, or facilitating foreign interference.

Question: What types of incidents are tracked based on the underlying intent?	1-10	11-20	31+
Accidental	53%	0%	6%
Negligence	47%	6%	18%
Malicious	29%	6%	6%

**Percentages do not equal 100, and only represent incidents that are reported by organizations*

An interesting finding concerns the types of incidents that are reported. Insider threat incidents due to negligence exceeds those caused by accidental or malicious threats. This is not a trend that is always observed in industry reports, and suggests that negligence, as another category of insider threat, may be more common than accidental threats.

Different types of insider threats may result in the following **outcomes:**

Data exfiltration

Theft or compromise of sensitive data developed/ supported by an organization (e.g. intellectual property, financial markets data, personal identifiable information)

Fraud

Use of position or access to data to intentionally deceive their organization for personal gain (e.g. embezzlement, procurement fraud)

Sabotage

Actions that put critical infrastructure at risk through purposeful sabotage of assets (e.g. introduction of malware, manipulation of databases/ backups, physical destruction)

Workplace violence

Acts of bullying, harassment or violence or the threat thereof, against employees by a coworker

Foreign interference

Collusion with foreign nation states to undermine national security/ sovereignty (e.g. theft of classified information or emerging technologies, favoring foreign suppliers)

Ideologically motivated violent extremism (IMVE)

IMVE can stem from a broad range of causes—including political extremism, religious radicalization, or social grievances—and often individuals, groups, or institutions perceived as opposing the extremist's worldview

A comprehensive approach that tracks insider threat activity along the spectrum from accidental to negligence to malicious is vital for several reasons.

By monitoring and categorizing incidents across the spectrum, organizations can spot patterns before they escalate. Many malicious acts begin as policy violations or repeated errors. Identifying these early—such as a history of negligent data handling—enables timely interventions like targeted training, enhanced supervision, or access restrictions, reducing the likelihood of escalation into intentional harm.

Tracking across all categories provides a complete view of the organization's human risk profile. Focusing only on malicious acts ignores the significant impact of accidental and negligent incidents, which often cause just as much operational and reputational damage. A spectrum-based approach ensures that leadership understands the interconnectedness of human error, carelessness, and intentional misconduct.

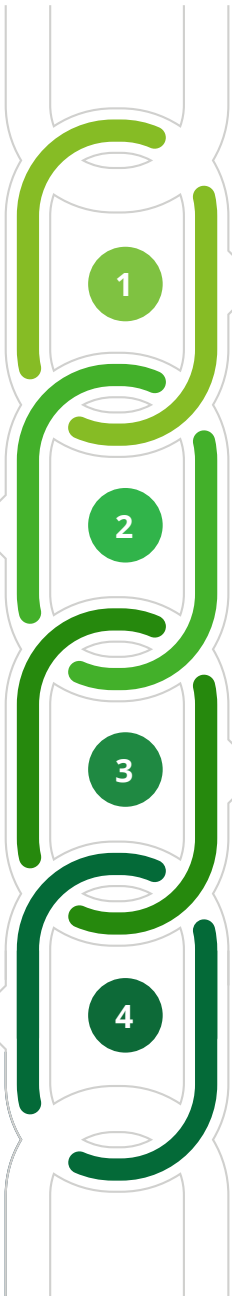
Finally, different threat types require different responses. Accidental incidents may be best addressed through awareness campaigns and process improvements, negligence through accountability measures and strengthened controls, and malicious behaviours through investigative and disciplinary actions. A structured tracking approach allows the organization to align the right countermeasures with the specific insider risk type.

By understanding the spectrum of insider risks, organizations can integrate cultural, procedural, and technical controls that protect both assets and people. This layered approach not only reduces vulnerability to internal threats but also reinforces trust between employees and leadership, building a security-conscious culture that naturally deters harmful behaviours.

Have you experienced the following:	Yes	No/decline to answer	Unknown
Personal information theft (data exfiltration)	76%	6%	18%
IP theft (data exfiltration)	59%	18%	23%
Fraud	53%	35%	12%
Sabotage	35%	47%	18%
Workplace violence	35%	41%	24%
Foreign interference	24%	47%	29%
Ideologically motivated violent extremism	12%	65%	24%

The results still show the wide variety of insider threats organizations face, ranging from data theft to much more serious issues related to national security and even radicalization. There were 76% of organizations that reported at least one incident related to personal information (PII) theft, while 59% of organizations reported an incident related to intellectual property (IP) theft. Combined, these cases of data exfiltration often involve unauthorized access to sensitive client or employee data, as well as the misappropriation of proprietary designs, trade secrets, or research. The frequency and impact of such incidents underscore the critical need for robust access controls, continuous monitoring, and employee awareness programs to safeguard personal and corporate assets from insider threats.

Organizations are strongly encouraged to agree on a common definition of insider threats so that security program leaders can better communicate the extent of risks to executive leadership, which will facilitate obtaining resources and investments for managing these threats. A common definition of insider threat provides the foundation for an organization to enhance its capabilities to detect and respond to insider threats.



COMPREHENSIVE ENTERPRISE - LEVEL RISK MANAGEMENT GOVERNANCE AND PROCESSES

Governance across all enterprise lines of defence, establishing an operational "insider risk hub"

CENTRALIZED DATA COLLECTION, MULTI-DISCIPLINARY ANALYSIS

Behavioural research, change management, cybersecurity, data science, risk management

USE - CASES BASED ON PAST COMPROMISES, INDUSTRY FRAMEWORKS

Identify potential risk indicators (PRIs) for the organization, consider industry models (e.g., MITRE Enterprise Att&ck)

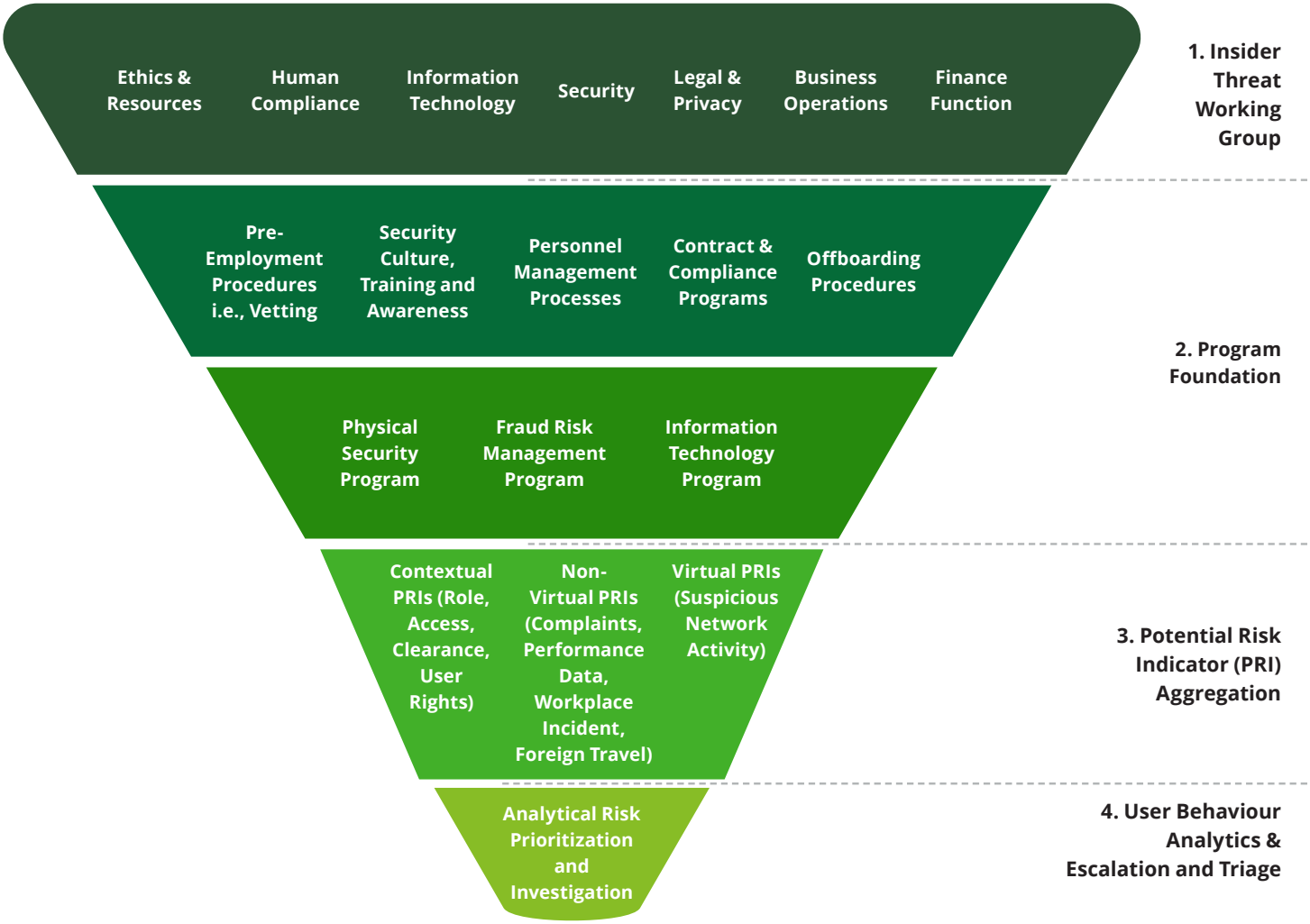
CONTINUOUS AWARENESS AND TRAINING

Communicate to the broader employee base and enhance security practitioners' technical skills, and promote best practices, policies, and lessons learned when an insider threat compromise occurs

Mitigating insider threats

Insider threat mitigation, with people and behaviour as the focal point, requires a broad approach. On a daily basis, people will interact with their organization in many different ways – physically and virtually, individually and in groups. It is therefore necessary to consider controls across all elements of the workplace and throughout the employee lifecycle.

The framework below organizes the functional components necessary for an effective, holistic, risk-based insider risk management program. This structure incorporates the governance and oversight, identify, protect, detect, respond, and recovery framework, capitalizes on existing capabilities, and promotes stakeholder coordination. This approach transcends the traditional focus on technology and takes an approach that is inclusive of business processes, policies, technology, and training.



The four key elements of an Insider Risk Management Framework

1

Insider threat working group

Cross-functional stakeholders with a shared understanding of insider threat who set risk culture and are accountable for insider threat programmatic direction.

2

Program foundation

Preventative controls throughout the employee lifecycle that begin to integrate traditional physical security and cybersecurity domains.

3

Potential risk indicator (PRI) aggregation

Identify potential risk indicators (PRIs), which are the behaviours, actions, events, and conditions that typically precede an insider threat act. Understand how PRIs are collected in data, where that data resides, and address legal and privacy concerns associated with data aggregation.

4

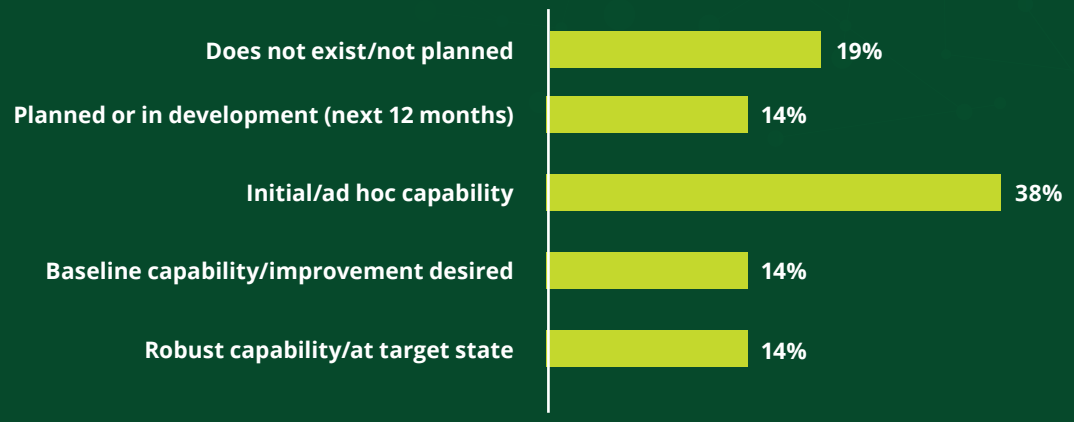
User behaviour analytics, escalation and triage

Following a risk-based approach, collect, correlate, and visualize PRIs from a variety of sources to proactively detect emerging insider threats. Individuals with elevated risk scores should be the focus of risk mitigation efforts subject to a standard and consistent escalation and triage process.

Deloitte asked survey participants to answer ten control focused questions aligned to this framework. Responses and commentary are found on the following pages (pages 15-24).

Insider threat working group/steering committee

Does your organization have a dedicated insider threat working group (or similar cross-functional group) that meets on a recurring basis to discuss insider threat risks, trends, and organizational vulnerabilities, and to guide insider threat mitigation strategy across your organization?



The percentages of responses to different control areas that are subsequently outlined, are based on the responses obtained (n=21); 34% of respondents did not answer these questions.

> "We are working toward the establishment of a formal Insider Risk program. During our initial process, we have established an ad-hoc working group that is intended to identify key areas at risk and lay the foundation of a response protocol. The working group is also allowing for discussions on immediate gaps such as employee screening as well as awareness and capacity building initiatives. We are a long way from where we hope to be in the future but it's starting to gain some traction."

Coordinated **insider risk management governance**, through a dedicated working group, is critical to effectively managing insider threats. Only 14% of organizations indicated that they had in place a robust cross-functional working group to coordinate efforts related to internal threat management. This means that even though many organizations have security controls and mechanisms in place, these often operate in isolation, within different silos.

An insider risk management working group is important because insider risk touches many different parts of an organization and cannot be effectively managed by a single function alone. A cross-functional working group provides the structure and forum to coordinate activities, share intelligence, and align priorities across business units such as security, cybersecurity, fraud, human resources (HR), legal, compliance, communications, privacy, and IT.

Cross-Functional Coordination

Insider threats often span technical, behavioural, and organization domains. A working group ensures that information flows between the teams responsible for monitoring systems, managing personnel, and enforcing compliance. This coordination reduces silos and increases the ability to detect risks early.

Unified Risk Strategy

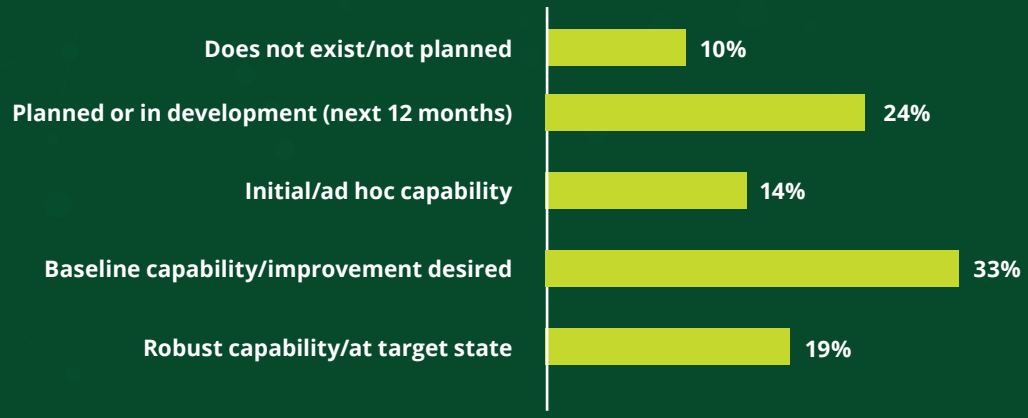
By bringing together stakeholders, the working group can establish a consistent definition of insider risk, agree on risk appetite, and ensure alignment with the organization's broader enterprise risk management framework. This avoids fragmented responses and supports executive reporting.

Culture and Communication

Insider risk is as much about culture as it is about controls. A dedicated group can work with communications and HR to socialize the program, promote employee awareness, and ensure interventions are balanced with trust and respect for privacy.

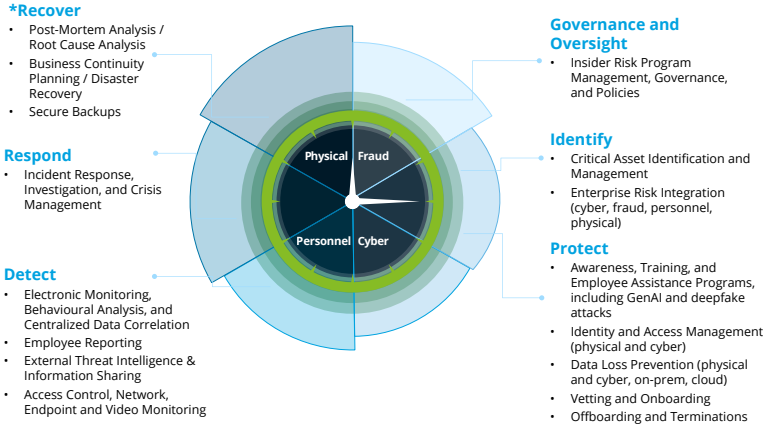
Insider threat policy and frameworks

Does your organization have an internal policy/framework that specifically addresses insider threat, including details of risk owners, escalation pathways and incident management responsibilities?



An **insider risk management policy and associated control framework** is important because it provides the foundation, consistency, and accountability required for effectively addressing insider threats across an organization. Without a clearly defined policy and structured framework, efforts to mitigate insider risk can become fragmented, reactive, or inconsistent across business units.

Our results display that more than half of Canadian organizations have concrete plans to strengthen their insider risk management policies and frameworks in the coming year. A quarter of respondent organizations already have policies and frameworks dedicated to insider risk management that is in the planning or development stages, while a third of organizations believe they already have basic capabilities to manage insider threats but would like to improve their programs.



Common insider risk management framework control elements that should be referenced in a policy

Establishing Clear Expectations and Governance

A formal policy sets out the organization's stance on insider risk, clarifies definitions, and articulates the principles that guide acceptable behaviours. It signals to employees, contractors, and stakeholders that insider risk is taken seriously and subject to oversight. Coupled with a governance framework, it ensures accountability, assigns responsibilities, and escalation paths when risks are identified.

Standardizing Controls and Practices

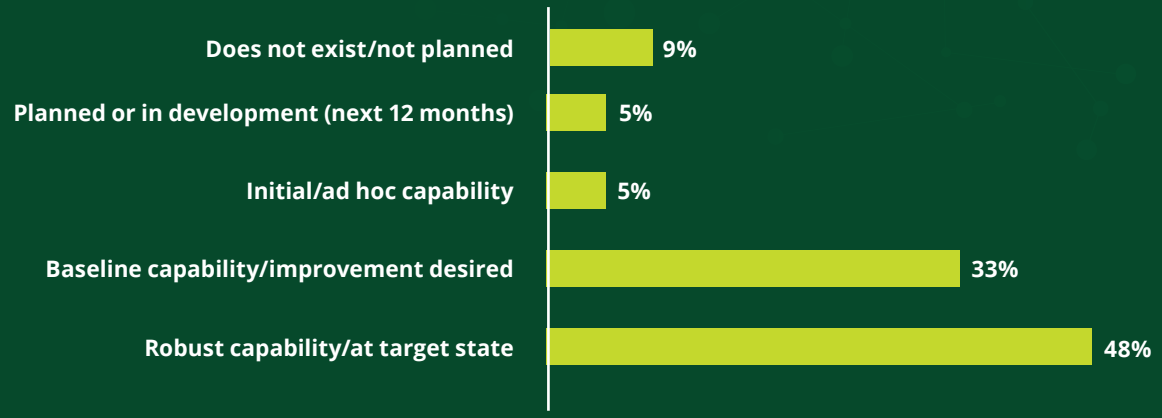
An associated control framework translates policy into actionable measures—such as access controls, monitoring, behavioural analytics, training, and response protocols. Standardization ensures that insider risk is managed consistently, reducing the chance of blind spots. It also provides a structure way to balance monitoring and prevention with respect to privacy and employee trust.

Supporting Compliance and Resilience

Regulatory and industry guidance in Canada (Public Safety Canada, Canadian Centre for Cybersecurity, and OSFI) increasingly emphasizes proactive insider risk management. A policy and framework demonstrate compliance with these expectations and provide defensible evidence of due diligence in the event of an incident. This strengthens resilience not only against malicious actors, but also against accidental and negligent threats.

Pre-employment screening

Does your organization perform background checks as part of the pre-hire process, which may include criminal history checks, credit checks, social media checks and/or other specialised checks?



> “Private industry needs an avenue to perform more enhanced background checks on international contractors who require remote access to networks and systems. Standard criminal record checks through third party vendors only touches the surface. We need to be able to link into the RCMP, CSIS or Public Safety Canada in order to facilitate more enhanced foreign checks as part of our due diligence”

Pre-employment screening is important because it serves as a first-line of defence against insider threats, helping organizations make informed decisions before granting individuals access to sensitive systems, data, facilities, and personnel. One survey respondent highlighted a fundamental point about the need for better collaboration between the private sector and federal government to enhance due diligence processes in hiring.

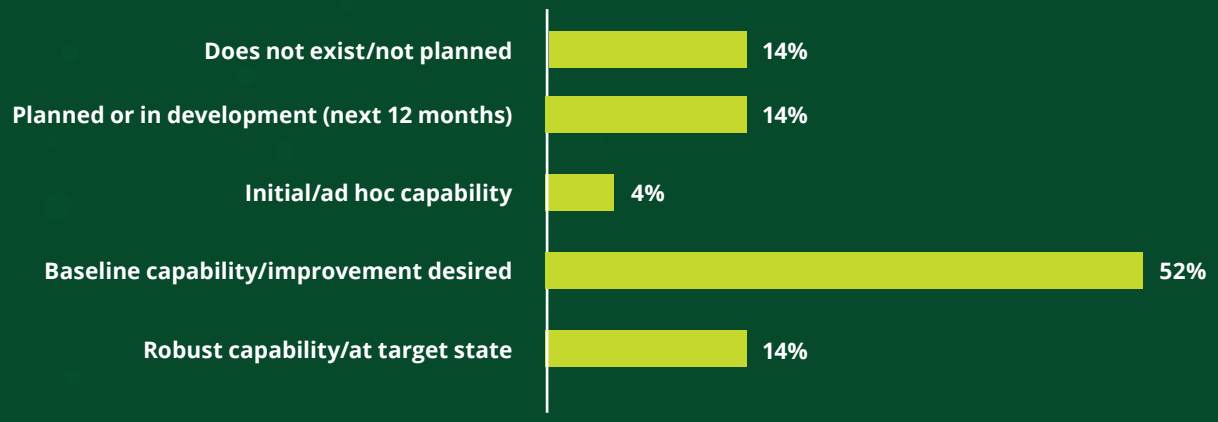
It is important to note that pre-employment screening is widely used within Canadian organizations, but it often remains limited to criminal background checks. A more comprehensive screening framework should include financial background checks and reviews of past behaviour in similar roles.

Pre-hire check types for consideration:

- Identity verification
- Right to work
- Employment history
- Education and credential verification
- Criminal record check (national, provincial, municipal)
- Credit/financial history
- Civil litigation records
- Reference checks
- Social media and open source
- Conflict of interest disclosure
- Foreign influence/interference screening
- Security clearance (for roles in government or critical infrastructure)

Ongoing/periodic assessment

Does your organization perform ongoing or periodic checks throughout the employee lifecycle, which may include criminal history checks and conflict of interest declarations?



The survey results display that the majority of respondents believe that improvements are required in the of conduct **ongoing monitoring and periodic reassessments** throughout the employee lifecycle.

Ongoing and periodic employee assessment following initial pre-employment screening is important because risk is no static—an individual's circumstances, behaviours, and access levels evolve over time, and so too does their potential risk profile. This is because circumstances can change—new criminal history, financial difficulties, and other changes in personal circumstances can alter individual behaviour and level of risk to the organization.

Risk Factors Framework

- Integrity and personal behavour
- Online activity, IT systems, and data security
- Personal or professional associations
- Criminal, statutory, and other judicial proceedings
- Finances
- Drug and alcohol use
- Personal stability and behaviour
- Loyalty to employer and foreign activity/influence

Canadian Insider Risk Management Centre of Excellence – Foundations for Screening and Risk Factors

Maintaining Security and Trust

Regular assessments reinforce a culture of vigilance and accountability. They demonstrate to employees that insider risk management is not just a "point-in-time" exercise at hiring, but an ongoing organizational priority. When implemented with transparency and fairness, this practice can strengthen trust in the organization's commitment to both safety and integrity.

Detecting Emerging Risk Factors

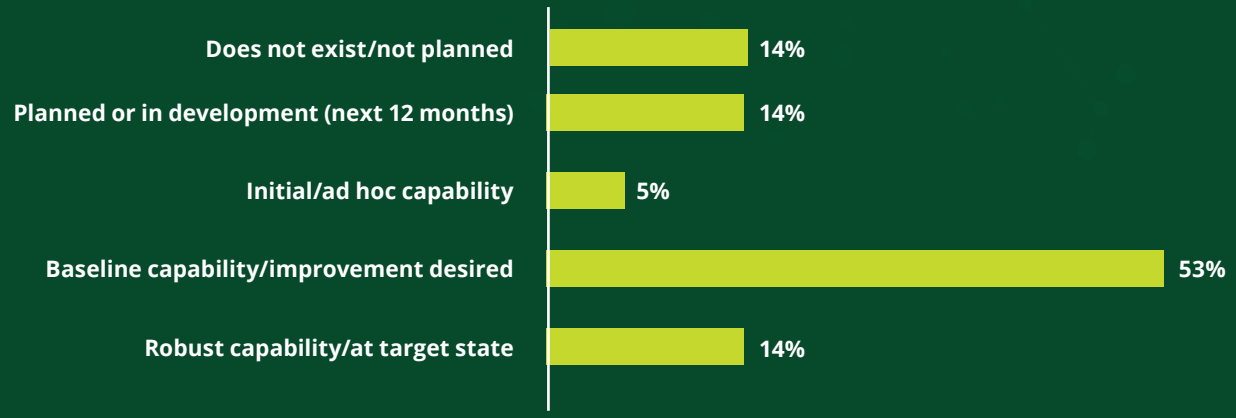
An employee who passed pre-hire screening may later experience changes in personal or professional circumstances—such as financial hardship, stress, grievances with management, or external pressures—that increase the likelihood of negligent or malicious behaviour. Periodic assessments help identify these emerging red flags before they manifest as insider threat incidents.

Adapting to Changing Roles and Access

Employees often transition into new roles, projects, or levels of responsibility, sometimes gaining elevated access to sensitive information or systems. Periodic reviews ensure that access remains appropriate and that individuals in high-trust positions continue to meet the organization's security and behavioural standards.

Insider threat training and awareness

Does your organization have internal training and awareness programs that specifically address insider threat and may highlight common insider threat indicators and reporting channels?



In terms of training and awareness, it appears that annual compliance training focused on insider risks is becoming more widespread among Canadian companies.

Organizations are implementing some type of annual, mandatory training that is increasingly available in cybersecurity, and this type of training specifically dedicated to insider threats is expected to grow in the coming years.

The survey results suggest that more needs to be done to raise awareness of insider threats within organizations. This could include the sharing of case studies, training sessions, or lunch and learns that outline the real consequences of insider threats. Just as cybersecurity awareness is now commonplace and linked to compliance, dedicated training on insider threats should also become standard in organizations to make employees aware of these risks.

Staff Training Considerations

Insider threat training should focus on building broad awareness and instilling a culture of responsibility in day-to-day operations. Employees need to understand what insider threats are, how they can arise through accidental, negligent, or malicious behaviour, and the potential outcomes such as data exfiltration, fraud, or workplace harm. Training should emphasize practical actions, such as safeguarding sensitive information, recognizing suspicious behaviours, reporting concerns through appropriate channels, and adhering to security protocols consistently.

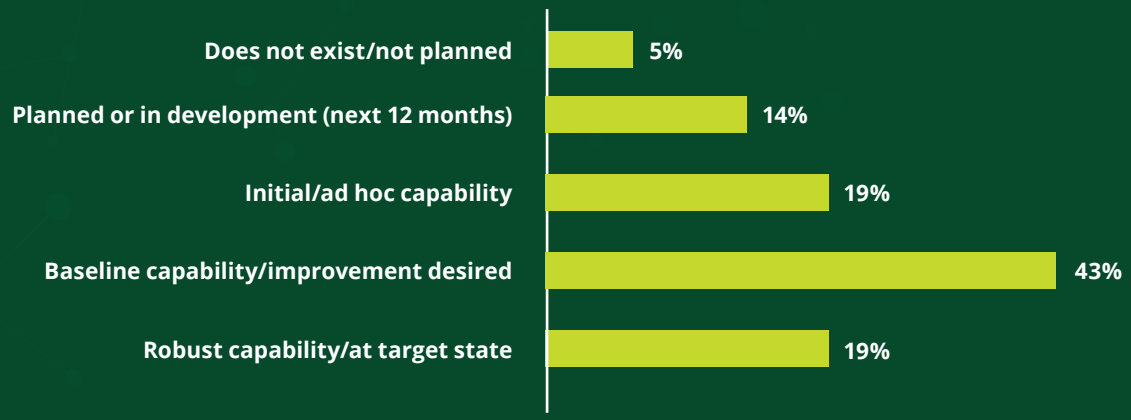
Since employees are often the first line of defence, awareness programs should also reinforce that insider risk is not just a security or IT issue, but a shared responsibility across the organization. To be effective, training must be accessible, non-technical where possible, and linked to real-world examples that make the risk tangible without fostering a culture of fear or mistrust.

Supervisor Training Considerations

Require more advanced and targeted training that goes beyond general awareness. They must be equipped to identify patterns of concerning behaviour, recognize early warning indicators, and manage sensitive situations with discretion and professionalism. Training should prepare supervisors to navigate the balance between employee privacy and organizational safety, including how to engage HR, legal or security functions when escalation is necessary.
Supervisors play a crucial role in fostering a culture of trust, ensuring their teams feel comfortable reporting incidents without stigma. Their training should cover regulatory responsibilities, the importance of documentation, and how to integrate insider risk considerations into broader operational oversight. By positioning supervisors as both role models and first responders, organizations ensure risks are managed consistently and proactively.

Offboarding procedures

Does your organization have procedures in place to specifically manage the risk of outgoing employees such as enhanced monitoring, an offboarding checklist and/or review of physical and IT access?



Offboarding is a critical component of insider risk management because it represents the point in the employee lifecycle where risk can be highest if not properly managed. When individuals leave an organization—whether voluntarily or involuntarily—they often retain access to sensitive information, systems, or networks that, if not revoked promptly, could be misused intentionally or accidentally. Whether voluntary or involuntary, employees who feel undervalued or dissatisfied may attempt to steal sensitive data or exploit assets for personal gain.

A large percentage of organizations have exit procedures in place, with 43% of respondents reporting that they have basic procedures and 19% reporting that they have more robust procedures.

Offboarding checklist for insider risk management

- Ensure the revocation of access and system controls
- Ensure the return and recovery of all corporate assets
- Conduct an exit scan of unusual data transfers or email forwarding in the weeks prior to departure
- Conduct structured exit interview
- Notify relevant stakeholders of departure
- Retain documentation of the offboarding process for legal, audit or regulatory review

Key considerations on the importance of employee offboarding

Protecting sensitive assets

Former employees, contractors, or third-parties may still have access to IP, customer data, or proprietary systems. A structure offboarding process ensures the timely revocation of access rights, retrieval of equipment, and safeguarding of confidential information to reduce the likelihood of data theft, fraud or sabotage.

Mitigating emotional or grievance-driven risk

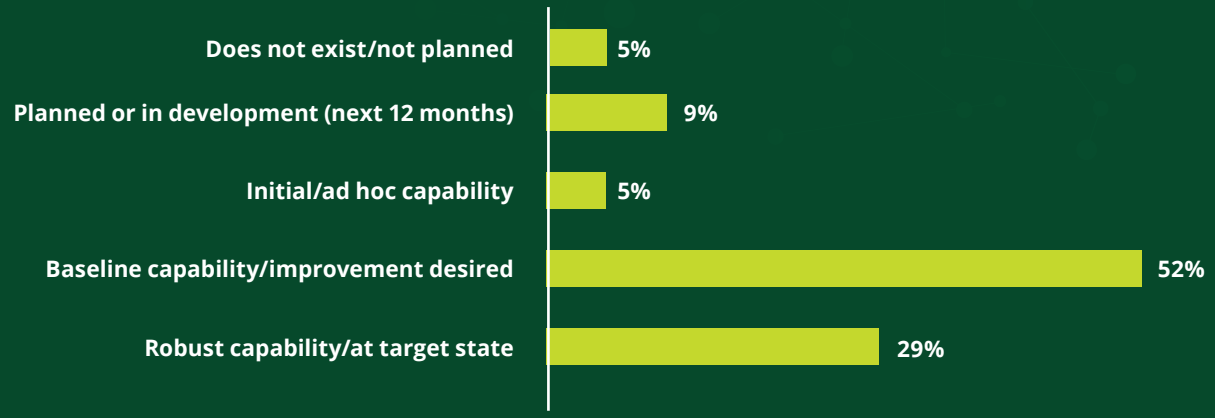
Departures can be emotionally charged, especially in cases of termination, restructuring, or disputes. Employees in these situations may feel resentment or a sense of injustice, increasing the likelihood of malicious actions such as leaking sensitive data or damaging systems. Offboarding processes that include respectful communication, clear expectations, and secure transitions help reduce these risks.

Culture and continuity

When offboarding is handled thoughtfully, it not only minimizes security risk but also maintains trust with remaining employees by showing that departures are managed professionally and respectfully. This helps preserve morale, reduce gossip or uncertainty, and reinforce a culture of accountability and security awareness.

Physical access management

Does your organization maintain physical access controls to manage the risk of personnel accessing restricted facilities or to identify irregular patterns of behaviour (i.e. physical access not required for job duties or outside of typical working hours)?



Among the areas assessed in this survey, **physical access management** emerged as one of the top domains where Canadian organizations reported having a robust capability at target state. Alongside pre-employment screening, physical access controls were consistently highlighted as a well-developed component of insider risk management programs. This reflects a long-standing emphasis on safeguarding facilities, sensitive workspaces, and critical infrastructure, where unauthorized physical access can pose immediate operational and security risks. The survey findings suggest that organizations are prioritizing the tangible, visible aspects of insider risk, with structured controls in place to manage entry, monitor movement, and maintain accountability in the physical environment.

Physical access management is important because it ensures that only authorized individuals can enter sensitive or restricted areas, reducing the likelihood of insider and external threats that could compromise people, assets, or information. It forms a foundational layer of insider risk management that complements digital and procedural controls.

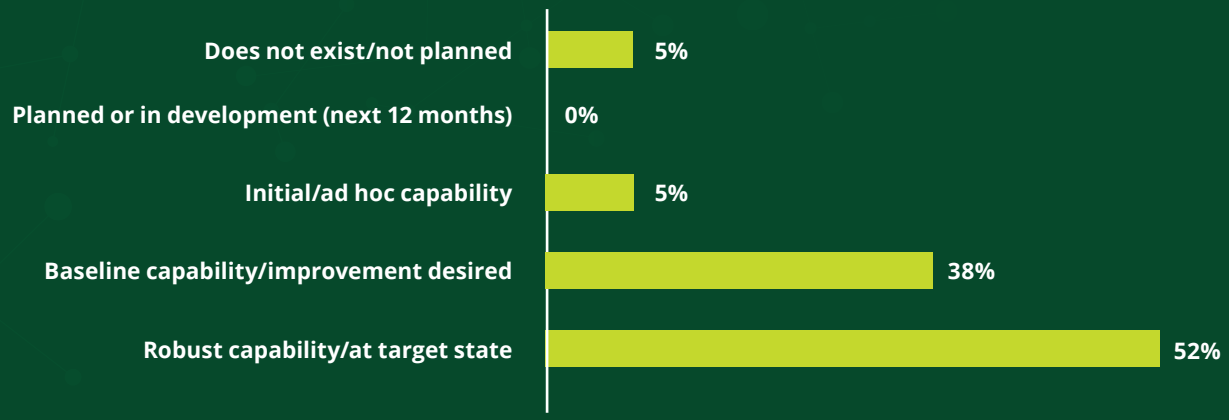
In today's interconnected environment, the boundaries between the physical and digital domains are increasingly blurred, making it essential for organizations to adopt a **cyber-physical approach to access management**. Treating physical and virtual access as separate silos can leave exploitable gaps. A unified approach not only strengthens resilience but also reflects the reality that modern insider threats often move seamlessly between physical and digital spaces.

Considerations

- **Protection of critical assets** - Controlling physical access prevents unauthorized individuals from reaching areas where sensitive data, IP, financial assets, or critical systems are stored. Even the strongest cybersecurity measures can be undermined if someone can walk into a server room or records archive without proper oversight.
- **Deterrence and accountability** – When employees and visitors know that entry and movement are monitored—through measures like badging, biometric authentication, or visitor logs—it deters casual policy violations and intentional misconduct. Audit trails also provide accountability, enabling organizations to trace who accessed certain areas and when, which is invaluable in investigations.
- **Integration with insider risk programs** – Physical access data is a valuable potential risk indicator (PRI). For example, an employee repeatedly accessing areas outside their job function, or entering restricted areas after hours, may signal elevated risk. Integrated with UEBA or security monitoring, these patterns can help identify early warning signs of accidental, negligent, or malicious behaviours.
- **Business continuity and trust** – By preventing sabotage, theft, or damage to physical infrastructure, access management safeguards business continuity. It also demonstrates to clients, regulators, and employees that the organization takes security seriously, reinforcing trust and reputation.

Virtual access management

Does your organization maintain controls to manage access to systems, networks, or other virtual environments such as a implementing the principle of least privileged access or separation of duties?



Virtual access management was identified as one of the strongest capabilities reported by respondents, with a significant proportion indicating maturity at the target state. This focus demonstrates that organizations recognize the critical role of controlling digital access in mitigating insider threats, particularly in today's environment of hybrid work, cloud adoption, and interconnected systems. Robust virtual access management ensures that users are granted the minimum level of access needed to perform their roles, while advanced monitoring and identity management tools provide assurance that sensitive data and systems remain protected. The higher percentages from the survey in this area show that Canadian organizations are actively aligning their digital access strategies with insider risk best practices, reinforcing the importance of secure access in both the physical and virtual realms.

What is Zero Trust?

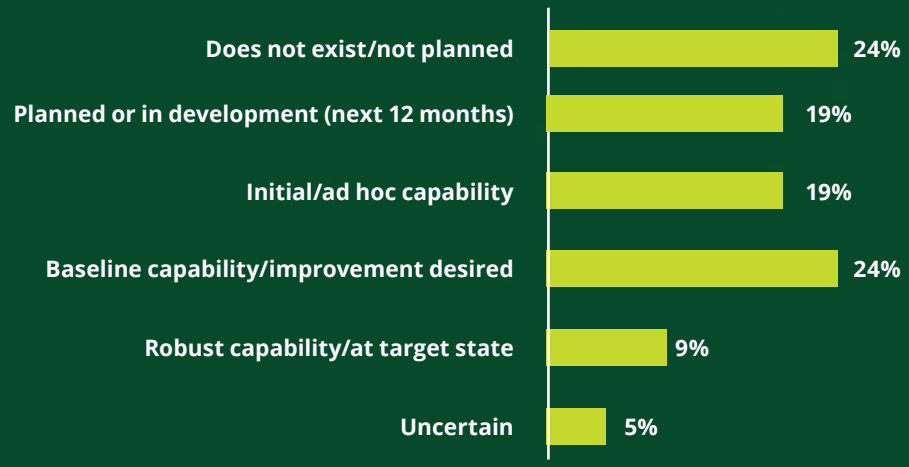
Zero Trust is a modern security approach built on the principle of "never trust, always verify." Instead of assuming that someone inside the organization or its network can be trusted by default, Zero Trust requires continuous verification of every person, device, and system request—whether physical (like entering a secure facility) or digital (like accessing sensitive data). Access is always limited to the least privilege necessary, monitored in real time, and revoked when no longer needed. By treating every access attempt as potentially risky, Zero Trust helps organizations reduce vulnerabilities, detect insider threats earlier, and build resilience across both physical and cyber environments.

Cyber-Physical for Access Management (Zero Trust lens)

- **Enforce least-privilege principles** – *Never trust by default* - Grant both physical and digital access only to the spaces, systems, and data required for an individual's role; review and adjust permissions regularly.
- **Continuous verification** – *Always verify* – Require identity verification at every point of access, whether entering a restricted physical area or logging into a virtual system, with multi-factor authentication (MFA) as a baseline.
- **Unified identity and access management** – *Zero trust architecture* – Treat physical and virtual access under a single Zero Trust identity model, where all access requests are authenticated, authorized, and encrypted.
- **Time- and context- bound access** – *Just-in-time and just-enough* – Implement temporary, revocable credentials for both facility visitors and third-party IT users, reducing standing privileges.
- **Segment and micro-secure** – *Microsegmentation* – Apply layered access protections to high-value zones (server rooms, executive spaces) and sensitive systems (financial or R&D databases), limiting lateral movement if a breach occurs.
- **Integrated risk monitoring** – Feed both physical and virtual access data into UEBA and SIEM tools, correlating anomalies across the cyber-physical spectrum to identify potential insider threats.
- **Employee awareness in zero trust culture** – Train staff to understand security is everyone's responsibility, emphasizing behaviours like preventing tailgating, safeguarding credentials, and reporting anomalies.

User and entity behavioural analytics

Does your organization employ user behaviour analytics (or a similar analytics solution) to augment detection capabilities by prioritising risky behaviour across the organization?



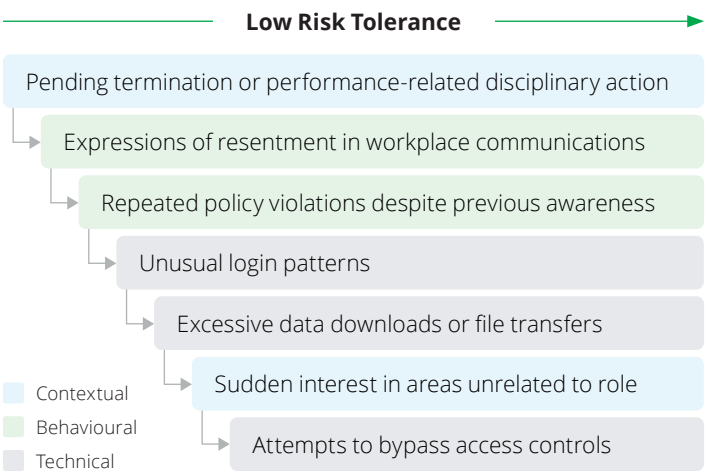
One of the most promising solutions in insider risk management is **user and entity behavioural analytics (UEBA)**, which are technologies that can detect abnormal behaviours which could indicate insider threats before they materialize.

Despite its potential, only 10% of respondents in the survey indicated that their use of UEBA was at an optimal level. This point connects to the finding that organizations are still largely reactive rather than proactive in their approach.

As the use of behavioural analytics in insider risk management increases, organizations are expected to become better equipped to detect suspicious behaviours. This will also enable better modeling of threats and risks and improve the overall posture of the organization against insider threats.

UEBA systems establish a baseline of "normal" behaviour for users and entities (such as accounts, devices, or applications) across the organization. They then continuously monitor activities—such as logins, data access, file transfers, and communication patters—to detect deviations from that baseline. When anomalies occur, UEBA tools correlate them with known technical **potential risk indicators (PRIs)**, like unusual data downloads, repeated failed login attempts, access outside working hours, or attempts to bypass security controls. A layered approach combining technical, observable behavioural, and organizational/contextual PRIs allows organizations to distinguish between benign irregularities and genuine insider threat activity.

Common PRIs

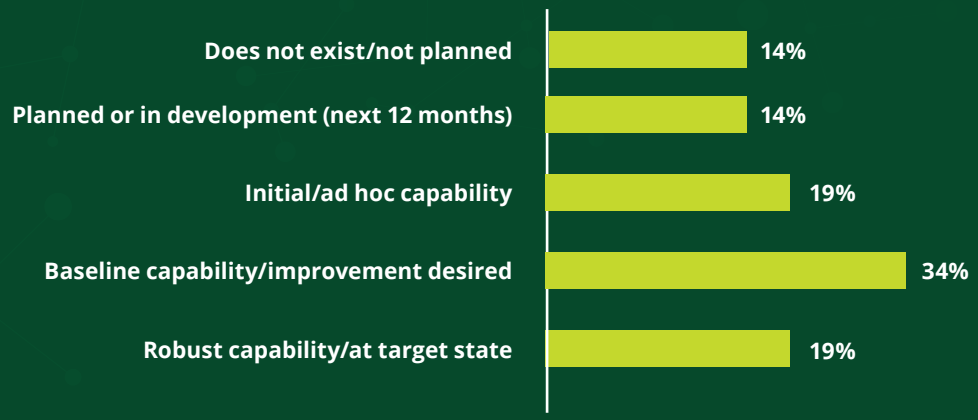


Is UEBA appropriate for my organization?

- If there are a large number of users, devices, and data flows, traditional monitoring may struggle to detect subtle anomalies when complexity makes it difficult to rely on static rules/alerts.
- If insider threats have been identified as a priority risk in your organization, UEBA can provide advanced detection and technical context to your existing PRIs.
- Ask whether current security information and event management (SIEM), data loss prevention (DLP), and identity and access management (IAM) tools provide sufficient visibility, or if they generate too many false positives.

Insider threat incident response

Does your organization maintain escalation and triage processes to manage the response to an insider incident, which may include defined roles and responsibilities and decision-making protocols?



Incident response is important because it ensures that organizations can move from detection to response action quickly and effectively, minimizing harm and preserving resilience when insider threat-related risks materialize. Unlike many external threats, insider threat incidents often involve individuals who already have trusted access, which makes both detection and response uniquely complex. A clear, structured response capability helps organizations manage this challenge in several key ways.

When it comes to incident response, only 19% of organizations have a formalized or robust triage and escalation process in place to respond to an incident related to an insider threat. About one-third currently have an ad-hoc capability in place and of that one-third, there are no additional plans to mature processes.

The low level of maturity is problematic, as insider threat incidents—whether accidental data leaks, negligent policy violations, or malicious acts such as fraud or sabotage—can escalate quickly if not contained. An incident response framework ensures immediate steps are taken to restrict access, secure critical systems, and protect sensitive data, reducing the scope and severity of impact.

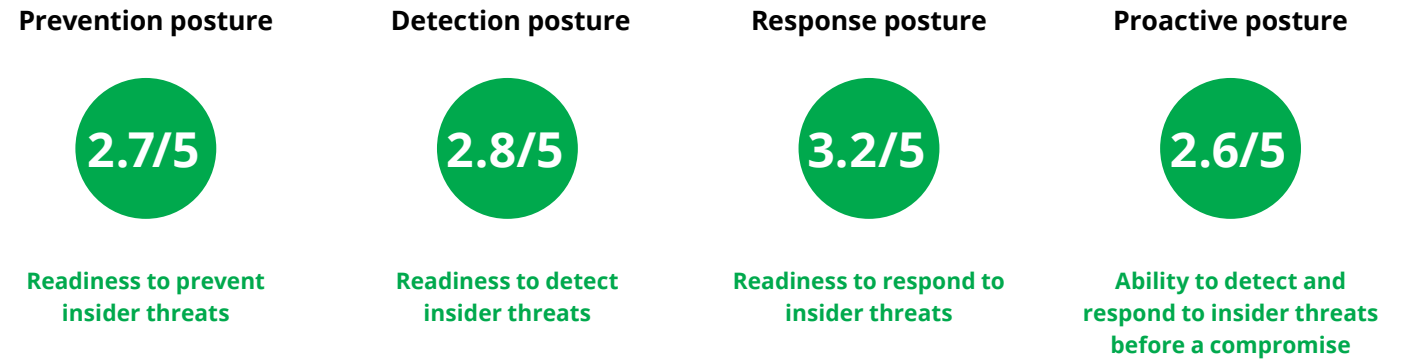
Additionally, without a defined process, responses to insider threat incidents are ad-hoc, fragmented, and delayed. A formal insider threat response plan coordinates efforts across HR, IT, legal, compliance, security, and leadership, ensuring each function knows its role and actions are aligned. This consistency reduces confusion and increases effectiveness under time sensitive conditions.

While effective incident response is critical, also consider the advantages of a proactive posture to insider risk management:

- Promotes transparency through communication and awareness on the nature of the organization's insider risk management program.
- Improves collaboration between different corporate and business functions within the organization.
- Centralizes insider risk management to manage increasing complexity in an ever-changing threat environment.
- Demonstrates the need for the organization to quantify current risks and the value of continued investments through increased visibility to senior executives and leadership.
- Improves detection and response through multiple IT tools, data collection, centralization, and risk modeling.
- Common definition and understanding of insider risk, impact, controls, and response prioritization based on the prior identification of critical assets and threat scenarios.
- Security awareness programs focused on accidental and malicious internal threats are implemented on a regular basis, followed by testing and corrective training for higher-risk business units.

Conclusion

Survey participants were asked to rate their organizations' overall readiness to prevent, detect, and respond to insider threats.



Looking at insider risk management trends, approximately half of Canadian organizations are generally more reactive than proactive when it comes to the mitigation of insider threats.

When we look at incident response capabilities, 48% of organizations rate their response capability at 4/5 or higher, making this one of the strongest insider threat controls.

In contrast, for detection, only 19% of organizations rate their capability as effective. For prevention, this stands at 24%. These results highlight a major challenge facing the industry: the shift in mindset toward proactive detection of insider threats.

Survey participants were asked to rate how proactive their organizations are in preventing, detecting, and responding to insider threats.

The results show that organizations still primarily respond after incidents occur, rather than implement enhanced detection and response controls, leaving them vulnerable to costly, disruptive, and avoidable insider threats.

While the results of the survey show that insider threats are a more prominent issue in Canadian industries compared to a decade ago, it is clear that significant efforts remain for organizations in terms of maturing various controls, as well as the need for strengthened legislation and standards (compared to the U.S. and Australia) to ensure that insider risk management norms are promoted across government, critical infrastructure, and private industry sectors.

The U.S. Government has required dedicated insider risk management programs in every government entity since Presidential Executive Order 13587 was signed in 2011. Since 2024, the Australian Government requires that dedicated programs are implemented in all government entities that administer security clearances as part of its Protective Security Policy Framework.

Perspectives for Canadian organizations

- Strengthen cross-functional coordination: Insider threat governance needs to be strengthened by creating dedicated working groups and cross-functional committees involving HR, IT, ethics and compliance, security, legal, and business operations.
- Accelerate policy development and implementation: Insider risk management policies must be developed and implemented. Clear guidelines on how to detect and respond to insider threats are needed to strengthen organization-wide commitment.
- Ensure continuous monitoring and integrate tools such as UEBA: The lack of continuous monitoring after hiring, with few periodic employee reassessments, exposes organizations to undetected risks. It is crucial to integrate tools such as user and entity behavioural analytics (UEBA) to identify risky behaviours throughout the employee lifecycle.
- Don't overlook behaviours outside digital systems: Insider threats often result from complex psychological and behavioural factors that don't manifest themselves solely on virtual platforms. Analyzing non-digital behaviors, such as in-person interactions and changes in employee habits, should also be a priority.

Appendix A: Guidance and regulation

In Canada, insider risk management is increasingly recognized as a critical component of organizational resilience. While not governed by a single, overarching regulation, insider risk touches multiple domains—security, privacy, fraud, and critical infrastructure protection—and is reflected in federal guidance, sector-specific requirements, and best practices. Canadian organizations must therefore take a multi-layered approach, aligning internal policies with national standards and regulatory expectations.

Public Safety Canada **Resilience to insider risk**	*Applies to: All organizations, focused on owners and operators of critical infrastructure* Outlines eight recommended security actions that can strengthen the resilience of organizational assets and systems.
Canadian Centre for Cybersecurity **How to protect your organization from insider threats (ITSAP.10.003)**	*Applies to: All organizations* *Provides several security procedures that can be implemented to reduce insider risks.*
Office of the Superintendent of Financial Institutions **Guideline B-13 Technology and cyber risk management**	*Applies to: Canadian financial institutions regulated by OSFI* *The focus of the guideline is to support financial institutions in developing greater resiliency against cyber and insider risks.*
Office of the Privacy Commissioner of Canada **PIPEDA Findings #2020-005**	*Applies to: Lessons learned and recommendations apply to all organizations in terms of balancing monitoring with employee privacy, to protect data* *"Provides recommendations concerning balancing employee monitoring and workplace privacy in the context of insider risk management.*
Innovation, Science and Economic Development Canada **Policy on Sensitive Technology Research and Affiliations of Concern**	*Applies to: Higher education institutions/universities* *Provides guidelines and tools to implement research security, including risk mitigation best practices focused on insider threats and research theft.*

Contacts

Pierre-Luc Pomerleau, Ph.D.,
Partner
E: ppomerleau@deloitte.ca

Victor Munro
Senior Manager
E: vmunro@deloitte.ca
Executive Director, CInRM CoE
E: victor.munro@cinrmcoe-cdecgrin.ca

Isabelle Fraser
Manager
E: ifraser@deloitte.ca

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 312,000 people make an impact that matters at www.deloitte.com.

As used in this document, "Deloitte" means Deloitte & Touche LLP. Please see https://www2.deloitte.com/ca/en/pages/about-deloitte/articles/about-deloitte-canada.html for a detailed description of the legal structure of Deloitte LLP. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2025 Deloitte & Touche LLP. All rights reserved.

Designed by CoRe Creative Services. RITM2225986