FIRPA

Practitioner Insights Report

November 2024

Brought to you by:

Australian Insider Risk Center of Excellence
Canadian Insider Risk Management Center of Excellence
United States Insider Risk Management Center of Excellence

Introduction

Insider risk management is an evolving field that requires continuous learning, collaboration, and adaptation to meet emerging threats. At the heart of building any robust practice is the sharing of experiences and insights among practitioners. Connecting professionals through an insider risk community of practice enhances our ability to mitigate insider threats by enabling the exchange of both common and novel challenges, as well as their solutions.

The Five Eyes Insider Risk Practitioner Alliance (FIRPA) is committed to fostering a global community of insider risk professionals through the Centre of Excellence hubs in Australia, Canada, and the USA. By creating spaces where practitioners can share their experiences, participate in training, and collaborate in workshops and conferences, we are building a global network of insider risk expertise.

Contributors

This report captures the insights of over 100 insider risk practitioners from Australia, the USA, and Canada who participated in a series of FIRPA facilitated workshops. Representing diverse roles and seniority levels across private sectors, government, defence, and academia, these experts provided nuanced perspectives on insider risk management, exploring seven key focus areas that have shaped the findings and recommendations outlined in this report.

Workshop Facilitators

The workshops were expertly facilitated by a team of experienced leaders, ensuring focused and productive discussions. Their guidance was essential in distilling the diverse insights and contributions from participants.

Facilitators:

- **Matt Salier**, CEO, Australian Cyber Collaboration Centre
- **Daniel Christiansen**, Learning Lead, Australian Insider Risk Center of Excellence
- **J.T. Mendoza**, Executive Director, US Insider Risk Management Center of Excellence
- **Victor Munro**, Executive Director, Canadian Insider Risk Management Center of Excellence
- **Josh Massey**, Director of Enterprise Risk, MITRE
- **Ben Cornish**, Director, McGrathNicol
- **Rajan Koo**, CTO, DTEX Systems

Approach

Through interactive, hands-on workshops, participants explored seven key themes in insider risk management:

01.	Stakeholder Engagement and Collaboration
02.	Security Culture and Leadership
03.	Education and Training
04.	Tools, Techniques, and Indicators
05.	Information Sharing and Collaboration Between Organisations
06.	Program Structure, Policy, and Governance
07.	Investigative Process, Procedure, Interventions, and Improvement

Each focus area includes three quick insights, and a summarised overview of the challenges and opportunities practitioners are facing. In addition to the seven focus areas, there are two further insights that were observed during the workshops including FIRPA Nation Nuances and Practitioner Surveys.

As you engage with this report, think of it as a source of inspiration—a guide to understanding the collective challenges and opportunities faced by insider risk practitioners. It's designed to encourage and support your own initiatives, offering insights that can spark new ideas and solutions for your organisation.

Please note this report does not include references to sources beyond the workshop summaries and insights.

Insights Summary

01.

Stakeholder Engagement and Collaboration: Securing executive buy-in and fostering cross-departmental collaboration is essential for successful insider risk management. Tailored communication and a shared lexicon can break down silos and align organisational priorities.

02.

Security Culture and Leadership: Leaders set the tone for a security-conscious culture. Open dialogue, transparency about incidents, and recognising security champions help create an environment where insider risk management becomes a shared responsibility.

03.

Education and Training: Blended learning techniques and real-world examples increase engagement in insider risk training. Continuous feedback ensures training remains relevant and effective in addressing evolving threats.

04.

Tools, Techniques, and Indicators: Advanced technologies like AI and behavioural analytics are transforming insider risk management, but must be complemented by an understanding of human behaviour to reduce false positives and enhance detection.

05.

Information Sharing and Collaboration Between Organisations: Legal clarity and governance structures are key to overcoming barriers to information sharing. Developing frameworks for sharing behavioural attributes from past incidents can strengthen industry-wide defences.

06.

Program Structure, Policy, and Governance: Clear governance frameworks, leadership engagement, and continuous improvement ensure that insider risk management processes are consistent and adaptable to emerging threats.

07.

Investigative Process, Procedure, Interventions, and Improvement: Clear escalation guidelines, post-incident reviews, and early involvement of legal and HR teams ensure investigations are compliant and lead to continuous improvement in managing insider risks.

a/ **FIRPA Nation Nuances:** Although common insider risk challenges exist across regions, key differences arise due to organisational environments and cultural attitudes. American practitioners emphasised ROI and advanced technologies, while Australian practitioners focused more on communication strategies, relationship-building, and aligning tools with organisational culture.

b/ **Additional Insights from Surveyed Practitioners:** Surveyed Australian practitioners identified negligence as the most concerning insider risk, highlighting the importance of education and collaboration in preventing unintentional threats. Practitioners also noted misconceptions about insider risk programs, stressing the need for clear communication to position these programs as protective, not punitive.

The first step is to identify the right people and get them involved from the beginning. Effective collaboration means connecting the dots across departments and building relationships early.

01. Stakeholder Engagement and Collaboration.

How can we engage stakeholders and foster collaboration across departments to create a unified insider risk management approach?

Executive buy-in is non-negotiable: Securing leadership support early is critical for driving insider risk initiatives and aligning organisational priorities.

Tailored communication breaks down silos: Clear, customised messaging across departments fosters collaboration and ensures everyone is aligned on insider risk management.

A shared lexicon fuels understanding: Establishing common terminology across the organisation creates clarity and helps unify insider risk efforts.

Effective insider risk management depends on early stakeholder engagement and cross-departmental collaboration. Securing buy-in from key stakeholders—particularly executives—ensures that insider risk initiatives are prioritised and supported from the top down. Clear communication, a shared lexicon, and real-life examples are critical tools in aligning various departments, including Legal, HR, IT, and Compliance, to create a unified approach.

However, challenges such as communication breakdowns, competing priorities, and a lack of shared understanding across departments can hinder progress. Many organisations struggle with defining insider risk in terms that resonate with non-security teams, limiting engagement. Resistance to change, skepticism about new security measures, and the absence of a common language make it difficult to foster collaboration and commitment.

To overcome these obstacles, organisations should focus on developing a shared language and tailoring communication to each stakeholder group, ensuring clarity and relevance. Engaging executive advocates early in the process can help drive a security culture from the top. By aligning goals across departments and using real-life case studies to illustrate the importance of insider risk, organisations can foster a collaborative and proactive insider risk management approach that is fully supported across all levels.

Collaboration between departments—joining forces, connecting the dots, and building relationships—can significantly reduce incidents and improve outcomes.

A positive messaging approach, celebrating wins, and fostering open dialogue is key to underpinning a strong security culture.

Executive awareness and leadership are crucial—when executives champion the cause, they set the cultural tone for the entire organisation, driving the security culture from the top down.

02. Security Culture and Leadership.

How can leadership drive a security-conscious culture and proactively manage insider risks?

Leadership sets the tone: Leaders must model security-conscious behaviours to embed insider risk management into the company culture.

Transparency builds trust: Open dialogue about security practices and insider risk incidents drives engagement and reinforces a positive security culture.

Recognise and reward security champions: Celebrating successes strengthens the security culture and encourages ongoing commitment from employees.

A robust security culture requires leadership to set the tone, making it clear that managing insider risk is a shared responsibility across all levels of the organisation. Leaders must lead by example, embedding security practices into daily operations and creating an environment where insider risk management is prioritised. Proactively addressing emerging risks, maintaining strict adherence to security protocols, and swiftly correcting lax security practices are essential for fostering a culture of feedback, accountability and vigilance in insider risk management.

Despite these efforts, organisations often face challenges such as silos between departments, biases in insider risk detection, and lack of buy-in from senior leadership. Security can sometimes be viewed as a lower priority or an inconvenience, leading to disengagement and non-compliance. Cultural differences across global teams can create gaps in how security practices are implemented and understood, weakening overall security posture.

To address these challenges, leadership must actively champion security, promoting a no-blame culture that encourages open reporting and engagement. Breaking down silos through cross-departmental collaboration, leveraging behavioural analytics tools, and aligning security initiatives with business goals are essential steps. By embedding security into the organisational fabric and promoting transparency, organisations can create a culture where managing insider risk is a natural part of business operations, supported by all.

Education isn't just about training. It's about trying different approaches, gathering feedback, and focusing on continuous improvement to keep the learning experience relevant and effective.

03. Education and Training.

How can we create engaging and effective training programs that build insider risk awareness across the organisation?

Blended learning boosts engagement: Blend multiple modes of learning delivery such as a combination of text, video, quizzes and project-based learning to keep employees engaged in insider risk management.

Real-world examples make training stick: Contextual, scenario-based learning helps employees understand the relevance of insider risk to their daily roles.

Continuous feedback sustains relevance: Regularly refreshing training based on feedback ensures that content stays engaging and effective.

Tailored security education and training are critical for embedding insider risk awareness across all levels of an organisation. Programs should leverage multiple modes of delivery and blend learning with static and dynamic approaches including real-life scenarios and simulations. By integrating insider risk education into existing initiatives, training becomes more efficient and resonant. Empowering employees with engaging, relevant content ensures continuous improvement and sustained attention.

However, cost constraints, lack of motivation, and outdated content often undermine the effectiveness of training programs. Companies also struggle to measure engagement and assess how well training translates into behavioural change. Without adapting training to the organisational culture and keeping it current, programs lose their impact. Additionally, over-reliance on data without actionable context leaves critical gaps in understanding insider risks.

To overcome these challenges, organisations must develop contextually relevant practices, invest in dynamic learning tools like scenario-based training, and ensure training remains current and engaging. Intermittent testing, such as phishing simulations, sustains employee engagement. A no-blame culture that promotes open communication, coupled with a shared language, builds alignment and trust across the workforce. When effectively executed, education and training will serve as a cornerstone for a resilient insider risk management strategy, positioning organisations to mitigate risks proactively.

Leveraging other teams and departments, like communications, can enhance the reach and effectiveness of training programs.

Before choosing tools and indicators, it's essential to understand your organisation—know what risks are relevant, how your culture impacts these risks, and what data you truly need. This understanding will guide your tool selection.

04. Tools, Techniques and Indicators.

What are the best tools and techniques for detecting and managing insider risks more effectively?

Data without context is a missed opportunity: Tools must provide actionable insights that align with the organisation's unique risk profile to be effective.

AI and behavioural analytics are game changers (if well utilised): Leveraging advanced technologies boosts detection capabilities and reduces false positives in insider risk management.

Human factors must guide tool selection: Understanding the motivations and behaviours behind insider risks ensures that the right tools are chosen to complement technical solutions.

Selecting the right tools and techniques is essential for effective insider risk management, but success hinges on aligning these tools with an organisation's unique risks and operational context. Before choosing any tool, it's critical to understand the specific insider threats an organisation faces and the cultural factors that influence them. By combining a deep understanding of human behaviour with advanced technical insights, organisations can develop a more nuanced approach to insider risk detection and response.

Challenges arise from over-reliance on data without sufficient context, difficulty integrating new tools with existing systems, and a lack of understanding of the human factors behind insider threats. Tools alone are not enough—without proper integration, regular reviews, and ongoing education, even the best technologies can fall short. Misaligned vendor tools and a focus on technology at the expense of human factors can result in gaps in detection and prevention efforts.

To address these challenges, organisations should focus on selecting tools that align with their specific risks and operational needs, ensuring they offer contextual accuracy. Implementing User Activity Monitoring (UAM) tools and leveraging AI and emerging technologies can significantly improve detection capabilities. Regular training and the development of internal experts on toolsets help maintain effectiveness and foster confidence in their use. When tools are integrated well and supported by strong organisational processes, they become powerful components of an effective insider risk management strategy.

It's not just about the technology—it's about understanding the tools, the education behind them, and the confidence they bring.

Teams need to manage internal incident data efficiently to make it readily available for external sharing without creating significant time burdens.

Organisations should task a governance council to oversee and facilitate information sharing between organisations. That creates progress, quickly.

05. Information Sharing and Collaboration Between Organisations.

How can organisations share insider threat information while addressing legal and privacy concerns?

Legal clarity unlocks collaboration: Engaging legal and privacy teams early removes barriers to sharing insider risk data and builds trust between organisations.

A governance council streamlines information flow: Establishing an active governance body ensures that incident data is shared securely and efficiently across organisations.

Behavioural insights drive collective defence: Sharing behavioural attributes from past incidents enhances collective understanding and strengthens industry-wide defences.

Sharing insider threat information between organisations is crucial but fraught with challenges. Legal barriers, privacy concerns, and organisational resistance often hinder effective collaboration. As insider risk perspectives evolve—particularly with the rise of blended attacks—organisations must recognise that risks can originate from, to, or through insiders. Overcoming these hurdles requires strong governance structures and early engagement with legal and privacy teams to ensure compliance and foster trust.

Challenges include reluctance to share sensitive data due to legal uncertainties, concerns over reputational damage, and difficulties in defining common terms for information sharing. Organisations also struggle with managing internal incident data efficiently enough to share it externally without creating a time burden. These barriers prevent timely, effective collaboration, leaving insider risk detection and mitigation siloed within organisations.

To address these challenges, organisations should focus on creating a common asset list, establishing legal-focused working groups, and promoting the sharing of behavioural attributes from past incidents. Developing an active governance council to oversee information sharing and refining common terminology will further enhance collaboration. With the right frameworks in place, organisations can work together to better understand and respond to insider threats, strengthening their collective defences.

Never waste a crisis—use it to drive home the importance of insider risk management.

Success in insider risk management requires a robust governance structure— one that clearly defines escalation and de-escalation procedures, effectively mitigates risks, and ensures incidents are reported to the Board with a focus on continuous improvement.

06. Program Structure, Policy, and Governance.

How can governance structures and policies guide consistent and effective insider risk management?

Governance frameworks ensure consistency: Clear policies and structured escalation guidelines create a reliable, repeatable insider risk management process.

Leadership engagement drives accountability: Securing leadership buy-in ensures that insider risk management remains a priority at all levels of the organisation.

Continuous improvement fuels resilience: Regular reviews and updates to policies ensure that the insider risk management program adapts to evolving threats.

A well-structured investigative process is essential for managing insider risks effectively, and this requires clear guidelines for escalation, well-documented procedures, and transparent decision-making. Implementing a double sign-off process for critical decisions ensures fairness and accountability. Engaging legal and HR teams early in investigations helps ensure compliance and protect the organisation's interests. Furthermore, continuous improvement through regular reviews and lessons learned keeps the investigative process robust and adaptive.

Challenges such as inconsistent executive support, resistance to change, and external pressures for compliance can hinder the effectiveness of an insider risk program. Many organisations struggle to integrate insider risk management into existing business practices due to competing priorities and a lack of resources. Additionally, reluctance to share lessons learned from incidents due to reputational concerns can prevent continuous improvement and limit the program's overall resilience.

To overcome these barriers, organisations should establish clear program frameworks with well-defined roles and responsibilities. Collaboration across departments and with external partners helps leverage expertise, while personalised approaches ensure relevance across different teams. Leadership buy-in is crucial, as is the development of a roadmap with measurable outcomes to track progress. When the program is supported by clear governance structures and a culture of transparency, insider risk management can become a shared responsibility across the entire organisation, ensuring both effectiveness and compliance.

It's crucial to establish clear thresholds for escalating incidents, document decisions thoroughly, and implement a double sign-off process for critical investigations to maintain fairness and accountability.

07. Investigative Process, Procedure, Interventions, and Improvement.

How can we improve investigative processes to ensure compliance and drive continuous improvement in insider risk management?

Escalation guidelines eliminate confusion: Clear thresholds for when and how to escalate investigations ensure consistency and prevent delays in responding to insider incidents.

Post-incident reviews drive learning: Root cause analysis and post-incident assessments are critical for improving processes and preventing future insider risks.

Legal and HR integration safeguards compliance: Early involvement of legal and HR teams ensures investigations are conducted in a compliant, risk-mitigated manner.

A strong investigative process relies on clear escalation guidelines, well-documented procedures, and a consistent approach. Implementing a double sign-off process for critical decisions ensures accountability and fairness. Engaging legal and HR teams early in the investigation process helps maintain compliance and protects both the organisation and individuals. Continuous improvement through regular reviews and lessons learned helps strengthen the process over time, ensuring it remains effective and aligned with organisational goals.

Challenges arise when investigative processes are inconsistent, when there is a lack of clarity around when to escalate incidents, and when balancing thoroughness with employee privacy concerns. These gaps can lead to delays, confusion, and missed opportunities to address insider risk incidents effectively.

To address these issues, organisations should focus on establishing clear guidelines for escalation, regular training for investigators, and using centralised tracking systems for transparency. Post-incident reviews and root cause analysis are crucial for learning from incidents, while celebrating investigative successes helps maintain morale and reinforce good practices across teams.

Post-incident reviews, including root cause analysis, are critical for continuous improvement and ensuring the health and wellbeing of your team.

a/ FIRPA Nation Nuances.

While insider risk management is a global challenge, the way practitioners approach these risks is shaped by regional contexts, organisational environments, and cultural attitudes. Through FIRPA's workshops, we've identified shared challenges across regions, but also notable differences in focus and execution between practitioners in Australia, the USA, and Canada. These distinctions offer valuable insights into how geopolitical factors and organisational cultures influence insider risk management practices.

Cultural Readiness and Resistance: In America, practitioners emphasised cultural resistance as a major challenge, with concerns about workforce hesitancy, information silos, and biases in insider risk detection. Overcoming these barriers requires focused efforts on fostering trust and promoting collaboration across departments. By contrast, Australian practitioners concentrated more on overcoming skepticism through clear communication and real-world case studies, indicating a slightly lower emphasis on broader cultural resistance.

Focus on ROI and Business Alignment: American practitioners placed significant importance on demonstrating the return on investment (ROI) of insider risk programs, consistently tying risk management efforts directly to business impact. This results-driven approach, with a focus on financial metrics, was a key differentiator. In Australia, however, the focus leaned towards relationship-building and strategic communication to win stakeholder buy-in, with less pressure on proving direct financial returns in the early stages of program implementation.

Technology vs. Human-Centric Approaches: In the USA, the workshop highlighted a strong focus on leveraging advanced technologies, including AI, behavioural analytics, and User Activity Monitoring (UAM), to stay ahead of insider threats. This tech-centric approach was positioned as critical for maintaining a competitive edge in detection and prevention. Australian practitioners, on the other hand, prioritised aligning tools with the organisation's culture and processes, placing greater emphasis on understanding human behaviour and ensuring technology complements rather than leads the overall strategy.

Bias and Siloed Risk Management: Biases in detection and risk management were more frequently highlighted in the USA workshop, where certain risk areas, such as cyber or fraud, were seen as receiving disproportionate attention. In contrast, Australian practitioners focused on overcoming communication challenges and fostering cross-departmental collaboration, with fewer concerns raised about biases or silos in their risk management approach.

b/ Additional Insights from Surveyed Practitioners.

During the Australian workshops on insider risk, more than 40 practitioners were surveyed with additional questions to explore key concerns and trends. The responses provided valuable data, highlighting three critical insights for advancing insider risk management.

1. Negligence: The Silent Insider Threat

Practitioners were asked which type of insider risk concerned them most in their organisation. The results showed that negligence, rather than malicious intent, is viewed as the primary threat. While malicious insiders and state-sponsored actors remain significant, the everyday mistakes and lapses in judgment by well-meaning employees are seen as the most pressing concern.

Survey Data:

Negligent: 53.8%	
Malicious: 30.8%	
State-Sponsored: 17.9%	
Accidental: 7.7%	

This finding emphasises the need for organisations to focus on reducing negligence through enhanced education, clear policies, and consistent training programs.

2. Education and Collaboration: The Foundation of Insider Risk Management

Practitioners were asked which individual skills or practices they felt were most critical for improving their insider risk programs. The responses highlighted the importance of continuous education and cross-departmental collaboration as foundational elements. Regular education keeps employees informed about emerging threats and their role in mitigating risks. When combined with real-world examples and interactive learning, training becomes more effective and relatable.

Additionally, the need for collaboration across departments, including HR, legal, IT, and security, was underscored. Practitioners agreed that breaking down silos and fostering teamwork across these functions is key to building a stronger and more resilient insider risk management approach.

3. Dispelling the Myth: Insider Risk Programs Aren't Punitive

Practitioners were asked what common misconceptions they expected to encounter about insider risk programs within their organisations. The most significant challenge identified was the misconception that these programs are punitive, designed to penalise employees or label them as threats. This perception, along with concerns that insider risk programs may be redundant or legally risky, could hinder their acceptance.

Top Misconceptions:

Insider risk programs penalise employees or label them as threats (35.9%).

Other departments already manage insider risks, making a dedicated program unnecessary (20.5%).

Insider risk programs create legal risks by profiling employees (17.9%).

To overcome these barriers, practitioners must clearly communicate that insider risk programs are protective and aligned with the organisation's goals, helping to safeguard both the business and its employees.

Other Misconceptions:

4. An insider risk program is counter to the organisation's culture (15.4%).

5. An insider risk program requires extensive new data collection on employees (5.1%).

6. Insider risk programs simply want more and more data (5.1%).

7. The organisation is secure from insider risks because it follows all regulatory and compliance standards (0%).

8. We cannot adequately address insider risks until we have the right tools (0%).

Conclusion.

Insider risk management is a continuously evolving discipline, that in the face of new and complex threats demands collaboration, innovation and agility to meet expectations. As highlighted in this report, securing leadership engagement, fostering cross-departmental collaboration, and balancing advanced technologies with human-centered approaches are critical to building a proactive and resilient insider risk program.

The insights gathered from over 100 practitioners across Australia, the USA, and Canada underscore both shared challenges and region-specific nuances. FIRPA's mission to foster a global community of insider risk professionals through its Centre of Excellence hubs is pivotal in addressing these challenges and enhancing practitioner expertise.

To succeed, organisations must apply the best practices outlined in this report—investing in leadership advocacy, tailoring communication strategies, and integrating both technical and human solutions into their risk management frameworks. By continuously refining these practices, organisations can stay ahead of evolving threats and bolster their defence against insider risks.

Now, the question is: What's your next move? We encourage you to take these insights forward—implement key takeaways, start conversations within your network, and engage with FIRPA's initiatives to continue learning and growing. As you build your insider risk practice, remember that as threats change and the critical strategies shift in response, FIRPA is here to support your journey with resources, workshops, and a global community of practitioners.

For more information about the Five Eyes Insider Risk Practitioner Alliance and to connect with our community, visit FIRPA.org.