Deloitte.

Insider Threat Management

A Deloitte South Africa point of view

Insider Threat Management helps organisations detect, prevent and respond to risks caused by people with legitimate access to assets, systems, data and intellectual property. It focuses on both intentional misuse as well as accidental or compromised behaviour.

Many loss incidents involve insiders, either directly or indirectly, and traditional fraud risk management does not address these types of risks. Regulatory pressure, remote work and increased data has made insider threats more likely and more damaging.

Types of insider threats

In a survey conducted between September 2024 and April 2025 by ***Deloitte Canada and the Canadian Insider Risk Management Centre of Excellence (CinRIM CoE)[1],*** data was collected Insider Risk practitioners on their perceptions of insider threats and their organisations associated controls.

The three types of threats where defined as follows:

1. **Accidental**
   Unintentional actions by an employee that result in harm or increased risk to the organisation, often due to human error, lack of awareness or misjudgment. Examples include sending sensitive information to the wrong recipient or mis-configuring a system without realising the security implications.

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

3. **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 such as data theft, fraud, sabotage, workplace violence, or facilitating foreign interference.

Outcomes

Different types of threats may result in the following outcomes:

- **Data ex-filtration:**
  Theft or compromise of sensitive data developed/ supported by an organisation (e.g. intellectual property, financial markets data, personal identifiable information).
- **Fraud**
  Use of position or access to data to intentionally deceive their organisation 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 of 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, favouring 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.

Mitigating Insider Threats

Mitigating insider threats requires a multi-faceted appraoch involving a cross-functional organisational framework that includes, but is not limited to:

[1] https://www.deloitte.com/ca/en/Industries/financial-services/perspectives/insider-risk-management.html

From a South African perspective, the survey findings re-inforce the following:

Insider threats are multi-faceted, encompassing accidental, negligent, and malicious actions.

Most incidents involve insiders - either directly or indirectly - underscoring the limitations of traditional fraud risk management approaches.

Economic pressures, remote work, and increased data volumes have amplified both the likelihood and impact of insider threats.

These insights suggest that organisations must adopt a holistic and proactive approach to insider threat management, moving beyond reactive or compliance-driven strategies.

Conducting a formal insider threat assessment and developing a defined insider threat management program delivers several tangible benefits:

- Comprehensive Risk Identification
  An assessment enables organisations to systematically identify risks arising from accidental, negligent, and malicious insider actions. This includes mapping potential outcomes such as data exfiltration, fraud, sabotage, workplace violence, and foreign interference.

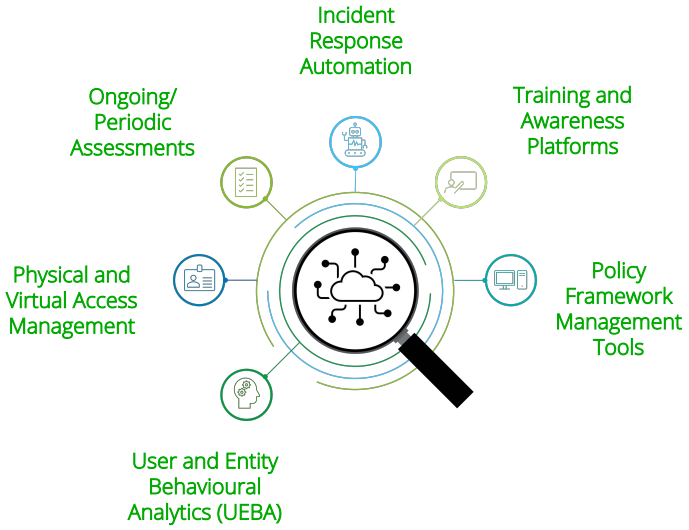
- Targeted Mitigation Strategies
  By understanding the specific threat vectors and their root causes, organisations can tailor controls and interventions—such as enhanced training for accidental threats or stricter access management for malicious intent.

- Regulatory and Stakeholder Assurance
  Demonstrating a robust insider threat management framework helps satisfy regulatory requirements and reassures stakeholders that the organisation is committed to safeguarding sensitive assets.

- Cultural and Behavioural Change
  Assessments often highlight gaps in awareness and compliance, providing a foundation for targeted training and a culture of vigilance.

- Incident Response Readiness
  Proactive assessment ensures that incident response plans are not only in place but are also informed by real-world risk scenarios, improving pipeline detection and response times.

A range of technologies can be leveraged to implement effective insider threat mitigation:



Insider threats are a growing concern, exacerbated by changes in working patterns and regulatory expectations.

A structured insider threat assessment, and maintenance program supported by advanced technology, is essential for identifying, mitigating, and responding to these risks. By adopting a holistic approach, such as combining policy, process, and technology, organisations can not only reduce the likelihood and impact of insider incidents but also foster a culture of security and trust.

It is important that all organisations consider not only whether these incidents could potentially materialise but rather when they will.

About Deloitte Risk, Regulatory & Forensic Services

Protecting tomorrow starts today.

From guarding against financial crime, to overseeing risk at every level, Deloitte can help you realise long term value through the protection of your business' integrity, investments and innovation.

Tailored solutions for Risk, Regulatory & Forensic

With increasing regulation and technology driven corruption, potential threats to the reputation and value of your business are widespread and continually evolving. We collaborate closely with you to help simplify and accelerate the building, operating and sustaining of right-sized risk and compliance capabilities whether in response to a specific event or planning for the future.

We combine global consistency with local market relevancy and offer deep inter-sectional knowledge across all industries to help achieve your organisations desired outcomes. Our meticulous approach to data management, experience with regulatory nuances and shrewd application of advanced technologies have earned us the trust of regulators everywhere.

Is it time you put your trust in us to?

Contact us

Dean Chivers
Partner
Africa Risk, Regulatory & Forensic Leader
E: dechivers@deloitte.co.za

Clayton Thompoulos
Partner
Africa Risk, Regulatory & Forensic
E: cthomopoulos@deloitte.co.za

Marlize Wentzel
Senior Manager
Africa Risk, Regulatory & Forensic
E: mwentzel@deloitte.co.za

Deloitte.