Deloitte.

Insider threat management in Australia

Findings from Deloitte's 2023 cross-industry survey

November 2023

About this report

This report details the findings from Deloitte Australia's inaugural Insider Threat Survey. Through this survey, Deloitte collected data from Australian risk leaders on their perceptions of insider threats and their organisations' associated personnel security controls.

The data in this report is informed by a survey conducted by Deloitte Australia between June and September 2023. The survey was completed by senior leaders including CROs, CIOs, CISOs, and fraud managers from a cross section of industries, and across ASX200 companies, Australian subsidiaries of foreign companies, public sector organisations, not-for-profit organisations and other privately held companies.

The data in this report is complemented by interviews with leaders across Australia and insights from Deloitte's own subject matter experts, with experience both in Australia 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, as well as Jayde Consulting and DTEX Systems for your support with this effort.

Foreword

Andrew Colvin, AO, APM
Partner
Deloitte Australia
Former Commissioner,
Australian Federal Police

In my current role as a partner in Deloitte Australia's Forensic practice, and as a previous Commissioner of the Australian Federal Police, I have experienced first hand the impact that malicious, ignorant, and complacent insiders can have on Australia's national security, critical infrastructure resilience, and business viability. As a country, Australia is relatively immature in its management of insider threats. We recognise the problem, but historically our approaches have largely been reactive. As this survey highlights, we may be effective in responding to the incidents we know about, but we need to do more – much more – to proactively prevent and detect these threats.

A range of legislation related to personnel management is helping to address this. This includes recent amendments to the Security of Critical Infrastructure Act 2018 (SOCI), which directs infrastructure asset owners to identify critical workers, assess their suitability and address risk arising from those workers. The new risk management programs that result from this legislation will undoubtedly improve our security posture. Importantly, however, my experience reinforces to me that insider risk management should never be viewed solely as a 'security problem'. A mature approach to managing insider risks starts with culture and 'tone from the top', supported by a multidisciplinary program that incorporates HR, legal, IT, operations, finance, and security functions to provide a holistic and balanced approach. A well-crafted, trusted insider program should mitigate risk while also creating an engaged and trusting workforce – a workforce where people are aware of insider threat indicators, empowered to support colleagues that show signs of distress, and have avenues to raise issues without fear of repercussion.

This report is foundational for Australia in that it is focused domestically and reveals how we prioritise and manage our people risks. It should give leaders cause to reflect on current practices in their organisations, integrate current capabilities, and consider what more can be done.

Michael Gelles, Psy.D.
Managing Director
Deloitte Financial Advisory Services LLP
Deloitte USA

As the former Chief Psychologist of the United States Naval Criminal Investigative Service and a leader of Deloitte's insider threat offering for the past 17 years, I have witnessed an evolution in the challenges that organisations face from their people. As we have moved from a world of bricks and mortar to one of bits and bytes, the context in which critical assets may be compromised has changed. While much of business is conducted on virtual systems the importance of continuing to observe anomalous behaviour outside of digital systems remains critical.

Clearly stated, the insider threat is a people-centric problem and the result of a number of psychological factors that contribute to the movement of an individual's behaviour along a continuum from idea to action. Today, many of these behaviours can be captured in data. Discernible risk indicators can be monitored, scored, and visualised to proactively identify and alert on potential nefarious or complacent behaviour.

Based on our extensive market experience in the United States and globally, mature programs today focus on a prevent, detect, and respond model that uses policy to align workforce activities to organisational risk tolerance. This is reinforced by communication and training, vetting across the workforce to include contractors and vendors, and sensitivity to separating employees. Information security is also paramount to effective mitigation. Technical controls can proactively interrupt the forward motion of an insider, protecting an organisation's most critical assets. Lastly, today's leading programs focus on employee well-being to drive an engaged and optimised workforce.

As emerging technologies such as Artificial Intelligence continue to shape the professional environment, program managers and leaders must continue to mature and evolve the protection of their critical assets. This report helps elucidate the need for a focused and pragmatic approach to identifying and mitigating vulnerabilities and will assist leaders in mitigating the insider threat.

Contents

Executive Summary

Most Australian organisations are only starting to consider the risks posed by trusted insiders. While awareness of insider threats is increasing at the executive level, many organisations still take a narrow view of this multifaceted and people-centric problem set. Recent legislation and regulatory guidance, driven by newsworthy insider incidents, has helped to raise the profile of the insider threat. For many organisations, however, the journey to understanding and successfully mitigating insider threats is only beginning.

Deloitte's anonymous survey of Australian risk leaders helps to shine light on the ways through which organisations address insider risk. In providing this benchmark against which organisations can assess their organisational readiness to address insider risk, five key insights have emerged.

1 Most Australian organisations have experienced an insider incident in the past year

Ninety percent of participating organisations have experienced an insider incident in the past 12 months. Few, however, were able to confidently quantify the volume of threats facing their organisation. Agreeing a shared definition for insider threat, and tracking incidents in line with that definition, will enable program leaders to effectively communicate the scope of insider risk with executive leadership.

2 Insider threat is narrowly defined, and cross-functional coordination is limited

Most organisations view insider threat through a narrow lens, with cyber and fraud teams most often 'owning' insider risk. Only 10% of respondents run a robust cross-functional working group to coordinate insider threat efforts across their organisations. Australian organisations must recognise insider threat as a people-centric issue where human risk can manifest itself in many different ways.

3 Australian organisations are more reactive than proactive

Incident response capabilities are the most robust of the insider threat controls discussed. While many participants noted some level of proactivity in dealing with insider threats, these efforts are narrow and ad hoc. Few organisations proactively address insider risk across their employee populations by understanding changes to individual risk profiles over time and intervening to correct concerning behaviour.

4 Pre-employment screening is common, but ongoing assessment is not

Ninety percent of organisations conduct some pre-employment screening – most commonly a criminal history check. However, most organisations end their external assessments there. This leaves many Australian organisations vulnerable to long-tenured employees who may experience changing circumstances over time (such as criminal activity, increasing debt etc.).

5 Data analytics is still in the hands of early adopters

Only 13% of survey participants stated that their use of user behaviour analytics (UBA) is at target state. Even these were primarily focused on virtual risk indicators. There is a significant opportunity for Australian organisations to develop and correlate non-virtual behavioural indicators to more proactively identify patterns and escalations in concerning behaviour.

Introduction

As Australia's professional environment continues to evolve, organisations face a broad and growing threat landscape. Business is increasingly conducted virtually, workforces are geographically distributed and technology-enabled, information is more accessible than ever, and third-party support is increasingly integrated into operations. But people, wherever and however they work, still drive organisational performance.

People, therefore, are an organisation's most important asset. But people are also human. We all have emotions, stresses in our lives, and we make mistakes. An insider incident occurs when these factors cause an employee or third-party to intentionally or unintentionally compromise organisational assets. Such compromises can cause irreparable damage to brand, reputation, and public confidence, and in cases of government institutions or critical infrastructure providers, threaten national security and public safety.

Recent high-profile incidents including accidental data breaches, intentional misuse of confidential information, and blatant fraud, theft and sabotage, erode public trust in Australian institutions and highlight the need for programs that coordinate organisational efforts to more proactively prevent, detect, and respond to insider threats.

Deloitte's 2023 Insider Threat Survey

The purpose of this survey has been to collect information from relevant executives to understand the nature of insider threats faced by Australia and the challenges faced by organisations in addressing these threats. The majority of survey questions focused on programmatic priorities and control capabilities associated with personnel security. The results presented in this report provide a benchmark for Australian organisations in assessing their organisational readiness to address insider risk.

An insider threat is an individual employee, contractor or vendor who, given their access to information, material, people, or facilities, has the potential to harm an organisation due to ignorance, complacency or malice.

About the participating organisations

30

Participating organisations

- 57% of organisations had fewer than 10,000 employees
- 43% of organisations had more than 10,000 employees

8

Industries represented

- Consumer Goods, Education, Energy & Resources, Financial Services, Healthcare
- Professional Services, Public Sector, Transportation

Qualitative and Quantitative

information captured during participant interviews

- 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 organisation over the past 12 months.

Ninety percent were certain that their organisation has experienced insider threats, however, few were able to confidently quantify the threat. Answers ranged from one to hundreds of incidents per year, demonstrating vast differences in how organisations define and track insider threats.

Throughout survey discussions, it became clear that many Australian organisations are only starting to consider the possible range of risks posed by their people. Insider threat definitions are inconsistent and often narrowly scoped to a single use case (e.g. data protection or internal fraud). Anecdotally, awareness and executive support is increasing, but many participants noted that investment in insider threat mitigation remains low in comparison to other risk initiatives.

90%

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

2.8/5

Overall awareness and understanding rating

3.2/5

Rating for insider threat as a priority

3.5/5

Rating for executive level support for insider threat

Defining and tracking insider threats

As illustrated above, an average insider threat awareness score of 2.8/5 demonstrates a low level of confidence in dealing with this people-centric issue. A key reason for this is the narrow view of insider threats that many organisations take. There is a perception that insider threat mitigation is predominately a cybersecurity challenge and categorised strictly as an information technology responsibility. Market experience has shown, however, that human risk is not contained to the virtual realm and that insider threats take many forms.

Data exfiltration

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 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)

While such threats may seem discrete and disconnected, taking a people-centric approach to mitigating insider threats puts observable human behaviour in the spotlight. Regardless of threat, malicious insiders move along a continuum from idea to action over time, leaving a trail of identifiable risk indicators. Even unintentional insiders are likely to exhibit risky behaviours prior to exposing organisational assets. A human-centric approach to mitigating insider threats, supplemented by a holistic program of technical and non-technical controls covering cyber, physical, and supply chain risks, provides organisations with the best chance to mitigate each of the above insider threats.

In practice, however, insider threat is often understood differently across disciplines. IT professionals are likely to define insider threat as aligned to employee interactions with IT systems and organisational data, while HR executives may view insider threats through the lens of workplace misconduct, bullying and harassment.

Survey participants were asked if and how their organisations track insider threats. The answers varied widely.

Among participating organisations, there was a high degree of variance in how insider threats are defined and tracked. That said, it is important to note that all threats discussed have been experienced in Australia.

> We have had misconduct, but nothing that has caused us material harm, so we wouldn't say we've had insider threat incidents under our classifications.

> The organisation is putting metrics in place now. At this point, I wouldn't want to hazard a guess as to what types of incidents we've experienced.

> I only have visibility of what is being investigated – serious misconduct – and we have a large caseload.

> I can only speak about confirmed frauds. And I wouldn't include bullying and harassment as an insider threat.

> As the cyber team we do some tracking, but there are probably things in this space that don't reach our team.

Have you experienced the following:	Yes	No/decline to answer	Unknown
Data exfiltration	47%	35%	18%
Fraud	43%	40%	17%
Sabotage	23%	53%	24%
Workplace violence, bullying and harassment	30%	33%	37%
Foreign Interference	10%	63%	27%

The significant rate of 'unknown' responses across threats demonstrates fragmented conceptions of what constitutes an insider threat. Such conceptions do not account for the holistic and multifaceted nature of how an individual interacts with the organisation they work for. It is critical, therefore, for organisations to define what insider threat means to them by considering the following:

Define your critical assets

Define and prioritise the organisational assets that are most critical to ongoing operations. Assets may include physical assets, people, facilities, customer information, and intellectual property (e.g. research and development data, source code, product designs etc.). Understand where these assets reside, especially data assets, which may be dispersed across your network environment.

Define your risk tolerance

Collectively define organisational risk tolerance associated with your prioritised assets. Determine what assets must be protected absolutely, as well as what you could afford not to protect. Gaining agreement on this will alleviate the need for your organisation to try to do it all, which often results in overwhelmed and unfocused security and investigative teams.

Align risk assessments to assets

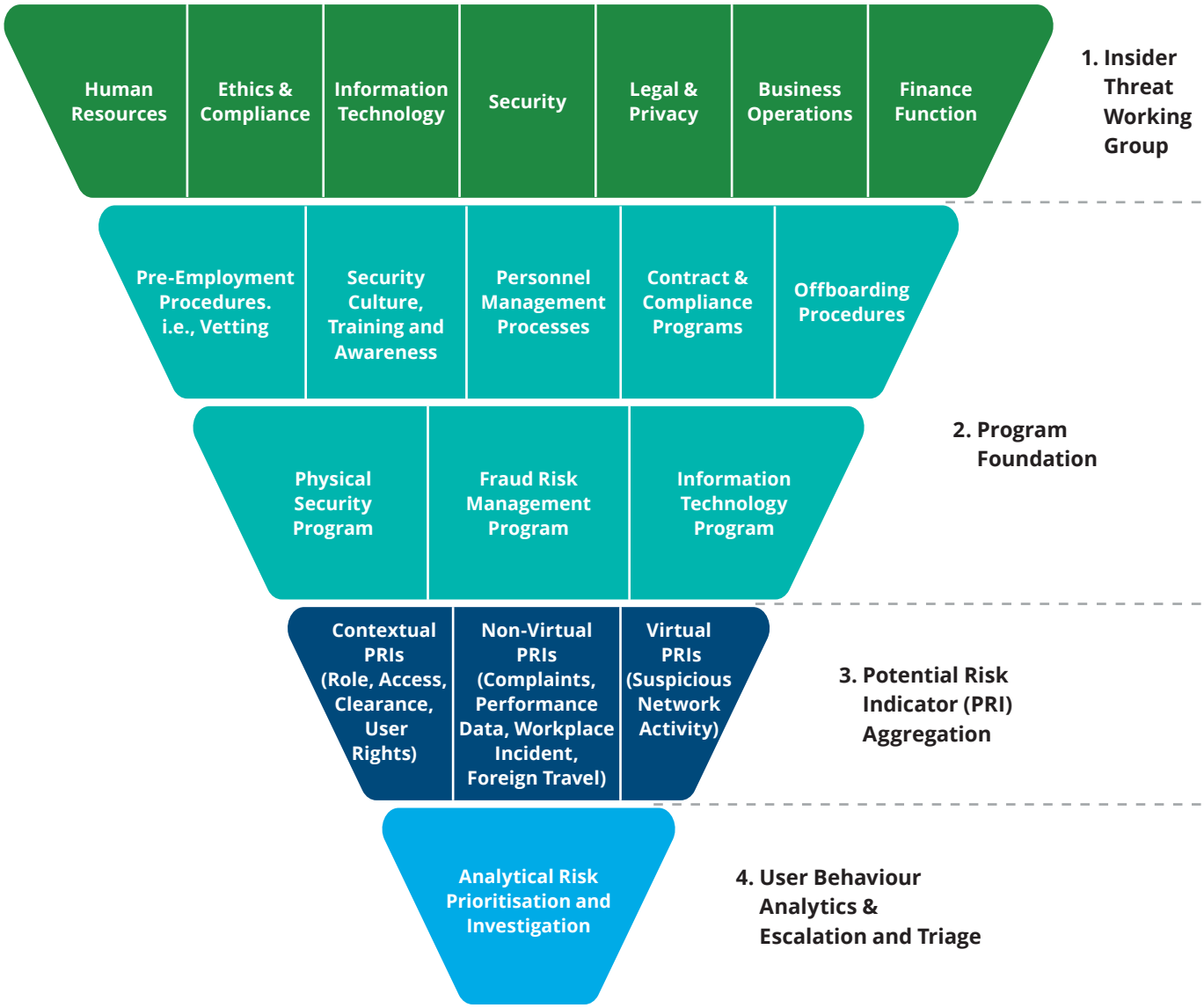
Understand the threats that are most likely to affect your prioritised assets. Define common use cases that highlight behavioural risk indicators and vulnerabilities within your control posture.

Once insider threat has been defined and scoped, organisations can most effectively track relevant incidents by type. Accurate tracking aligned to an agreed definition will enable program leaders to effectively communicate with executive leadership and develop business cases for investment. It will also allow organisations to align controls to commonly observed threats and behaviours. Organisations should take stock of existing controls and tailor capability development to address prioritised assets and threats while accounting for organisational culture. Too many security restrictions can impede an organisation's mission and workforce agility, while too few may increase vulnerabilities. Control capabilities, including employee monitoring, should align to risk tolerance and strike a balance between countering the threat and conducting business.

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 organisation 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 organises the functional components necessary for an effective, holistic, risk-based insider threat program. This structure incorporates the prevent, detect, and respond framework, capitalises 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 Threat 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 rndicator (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

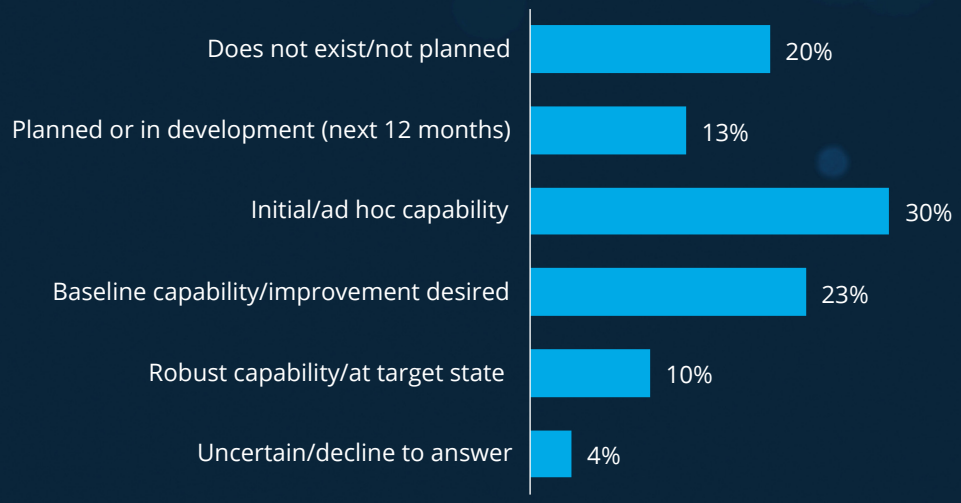
User behaviour analytics and escalation and triage

Following a risk-based approach, collect, correlate, and visualise 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 14-23).

Insider threat working group/steering committee

Does your organisation 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 organisational vulnerabilities, and to guide insider threat mitigation strategy across your organisation?



> Insider threat is part of a few different conversations, but I can guarantee we don't have a robust debate [on the subject].

> While we don't have a dedicated insider threat working group, we discuss insider threat incidents and controls within the context of a number of other risk committees.

Coordinated **insider threat governance,** through a dedicated working group, is critical to effectively managing insider threats. While survey respondents discussed the existence of many different control types within their organisations, these controls often operate in silos distributed across the organisation. Successful insider threat programs exhibit strong cooperation and information sharing, and view insider threat as a shared responsibility across the organisation. Mature insider threat governance should involve the following:

An insider threat working group is critical to defining and building the insider threat mitigation capability and securing the data, policies, and processes needed for the program. It should assist in addressing legal/privacy concerns and support the development of messaging to executives, managers, the broader employee population, and employee unions.

Executive support

Develop a cadence with executives and communicate program effectiveness. Drive buy-in that positions the program as an imperative.

Strategic foundation

Define critical assets and associated risk appetite. Align insider threat use cases to these assets to focus the program. Prioritise mitigation efforts on areas of greatest impact aligned to business strategy.

Ownership through a partnership model

Engage multiple disciplines to own critical components of the program. Develop an integration plan with key stakeholders to aggregate risk indicators and integrate escalation and triage processes within broader risk management capabilities.

Insider threat policy and frameworks

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

Clearly defined **insider threat related policy** is a key component of an effective insider threat program. When clearly communicated to employees and third-parties, policy sets the cultural tone by defining the behavioural expectations of your workforce. Policies, and associated frameworks, should both define acceptable behaviour and communicate clear consequences for violating policies.

Organisations may opt for a stand-alone insider threat policy or embed core insider threat considerations into existing policy documents. Both options have proven effective when adopting the following:

> We have things like a code of conduct and an IT usage policy, but they don't explicitly call out insider threat. We plan to improve in this area to align with SOCI requirements.

Clear communication

Embed policy into strategic communication campaigns that integrate with employee onboarding and are supported by training. Ensure all relevant policy is centrally located and easily accessible by staff.

Routine acknowledgement

To ensure staff understand policy, consider requiring policy acknowledgment both at the time of onboarding and at regular intervals beyond the initial acknowledgement.

Consistent enforcement

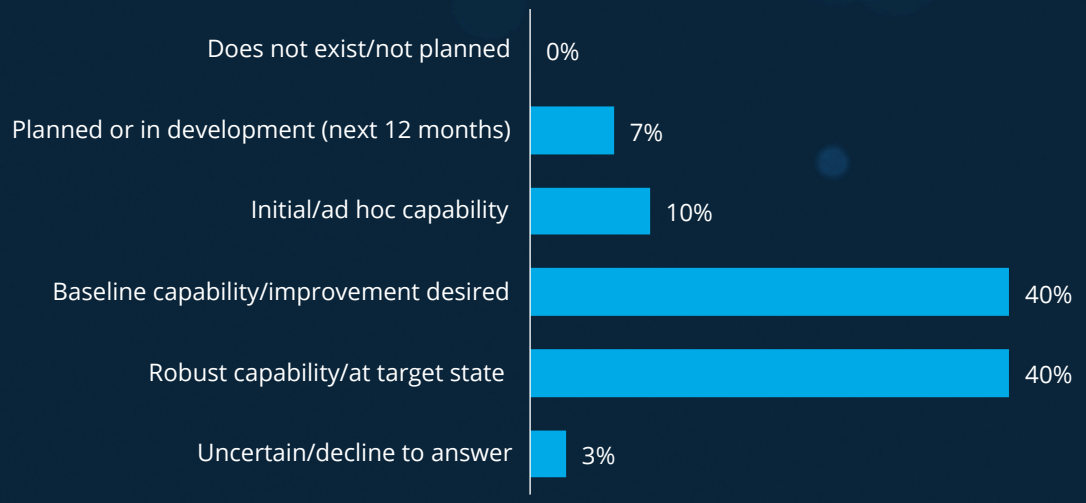
Consistent enforcement of policy is critical to establishing cultural and behavioural expectations. Compliance should be tracked and consequences for non-compliance should be clearly defined and consistently enforced.

Common insider threat policies/framework elements:

- Non-disclosure
- Acceptable use
- Intellectual property
- Data transfer
- Mobile device
- Removable media
- Social media
- Employee assistance
- Incident reporting

Pre-employment screening

Does your organisation 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?



> Pre-employment screening is mainly focused on police/ criminal checks. We don't look at credit or social media.

> It really depends on if the hiring manager wants to do it.

> It depends on the person coming into the organisation. We make risk-based decisions about what types of checks an individual needs.

Pre-employment screening is a core insider threat control, and the majority of survey respondents affirmed a baseline or robust level of employee vetting. Most responding organisations conduct criminal history checks at the time of hiring.

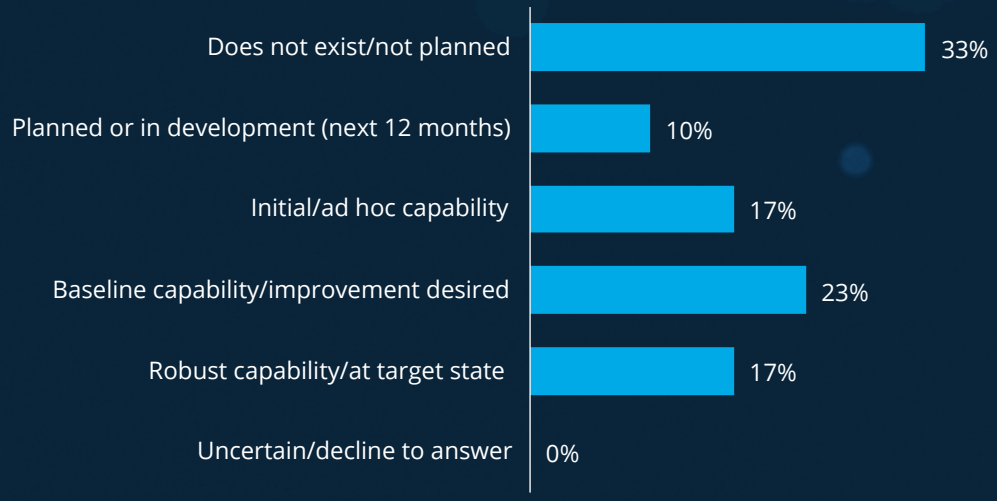
While broadening the scope of pre-hire vetting can help to identify red flags, it is important to engage legal and privacy teams in the decision-making process. Workers' rights and privacy must be considered and a risk-based approach to vetting is prudent and defensible. Many of the respondents who specified a robust capability in this area noted alignment of checks to risk-by-role frameworks.

Pre-hire check types for consideration:

- Identity verification
- Right to work
- Referees
- Education history
- Criminal record check
- Auscheck (critical infrastructure)
- Civil litigation records
- Digital footprint (network analysis)
- Bankruptcy check
- Credit reference check
- Employment history
- Traffic and driving records

Ongoing/periodic assessment

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



While pre-employment screening is commonly implemented across Australia, survey respondents were split on the use of **ongoing assessment** on employees. A significant portion of respondents do not conduct any periodic assessments and many of those stating a baseline capability noted only the use of conflict of interest declarations.

Periodic security assessments enable organisations to identify concerning behavioural changes over time and therefore help to increase proactive risk mitigation posture. As one survey respondent noted, post-incident investigations often reveal external risk indicators (i.e. recent criminal charges or dramatic increases in debt) that might have prompted proactive intervention ("We should have seen that coming.")

As with pre-employment screening, there are many checks that organisations may want to consider as part of ongoing assessments. Legal and privacy teams should continue to be involved in the decision-making process and ongoing assessment scope and frequency should be defined using a risk-based approach. Potential methodologies for ongoing assessments include:

> "We only do additional checks if an issue arises... sometimes we look back and say, 'we should have seen that coming'."

> "Certain positions require ongoing checks, but we don't do this for everyone – things do fall through the cracks."

Periodic assessments

Assessments conducted at defined intervals (e.g. annually) as defined by policy and communicated to staff.

Aperiodic assessments

Assessments conducted at irregular intervals with little forewarning provided to staff.

Continuous evaluation

Processes that leverage automated records checks and apply business rules to identify relevant risk indicators.

← **Moderate Risk Tolerance** — **Low Risk Tolerance** →

Insider threat training and awareness

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

Insider threat training is predominantly delivered at a baseline level in Australia. Survey respondents commonly noted that insider threat related content is embedded in existing training programs such as cyber security training, ethics and compliance training, and conflicts of interest training. Dedicated insider threat training, however, is less common.

Respondents were conflicted about the volume of training that should be required of staff, noting that increased training requirements can result in staff viewing training as a 'check the box' activity. While certain concepts should be covered for all staff (i.e. threats, observable indicators, reporting channels, privacy considerations), customised training based on role and risk is most effective.

> Do we have training on all aspect of IT risks – yes.
>
> Do we train specifically on insider threats – no.

> It's a tough one - training and awareness, you just can't do enough.

> "There are all sorts of trainings depending on the job function – safety, business compliance, corruption, etc. But how much training do our people have to suffer? We don't want them to sit at a computer just pressing a button to get through it.

Staff Training Considerations

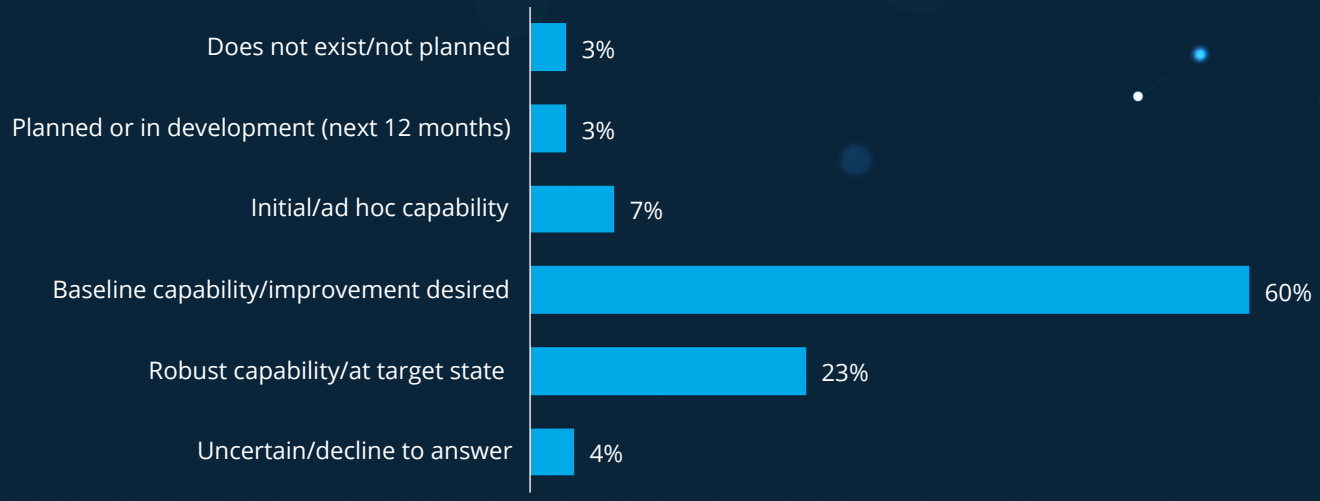
Organisations should educate all staff on basic insider threat concepts either through stand-alone training or embedded into an existing curriculum. Complement baseline training with role based-training and periodic communications aligned to security policy.

Organisations should develop supervisory training outlining how to best manage personnel who are demonstrating reportable behavioral indicators and the proper mitigation techniques to manage workplace incidents.

Supervisor Training Considerations

Offboarding procedures

Does your organisation 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?



Employee separations are often a trigger for insider activity. Whether leaving an organisation voluntarily or involuntarily, employees who feel undervalued may seek to use sensitive data or assets for their own personal gain. This makes the timeframe prior to separation an increasingly risky period and control posture should increase in line with the risk.

Fortunately, the vast majority of respondents noted baseline or robust **offboarding procedures.** Interviews with respondents, however, show that these results are nuanced. While almost all survey participants have some offboarding check-list in place, the effectiveness of these procedures is unclear. Multiple respondents noted a real concern about lagging access, but few employ enhanced account monitoring prior to or immediately following a separation.

> "We have a bunch of systems that aren't talking to each other."

> "We have very basic offboarding procedures – a checklist to recover hardware and building passes."

> "There are manual processes in place. Access reviews need some improvement. We've certainly had people with systems access after their departure date."

Respondents with confidence in their offboarding procedures noted strong cooperation between HR and security teams and a combination of the following controls:

Enhanced monitoring

Monitor online actions, particularly downloads one month before and after resignation.

Automated access removal

Automatically trigger removal of physical and virtual accesses at the time of separation.

Notifying colleagues

Communicate separations to colleagues and security personnel so that staff know not to disclose sensitive information to former co-workers.

Physical access management

Does your organisation 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)?

> We do have access controls, but we don't monitor it or identify patterns of behaviour.

> The head office is more robust with swipe card access, but for regional sites, it's just an old lock and key. The site manager looks after the key logs and secure boxes for these keys. Definitely, improvements are desired here.

All responding organisations noted some level of **physical access management** and while we have not provided a detailed industry breakdown of survey participants, it is worth noting that many of those who classify their controls as robust are critical infrastructure providers that manage sensitive physical assets.

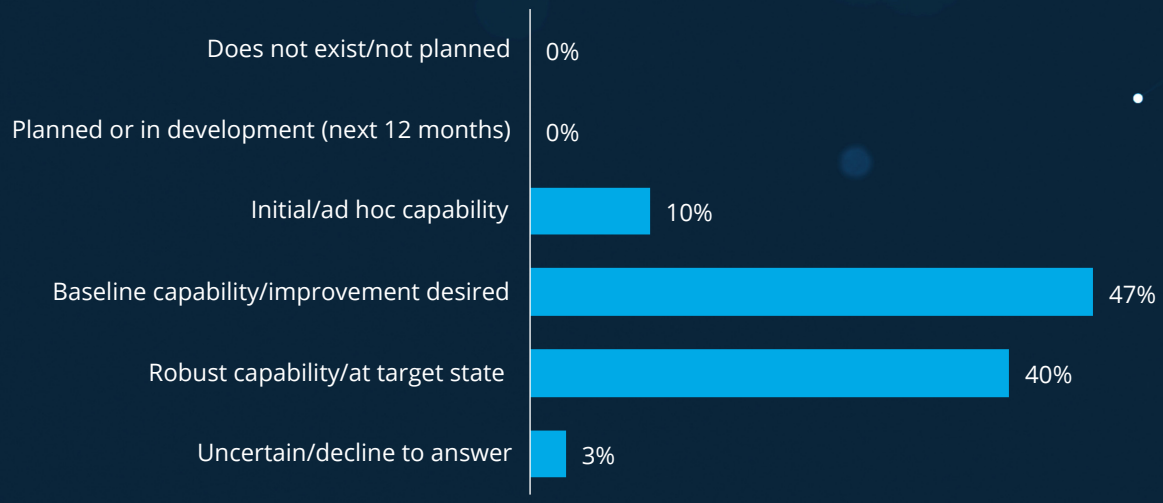
Many respondents, across all sectors, noted that controls are maintained and enforced inconsistently across the enterprise. In some cases, this aligns to risk-based decisioning (i.e. the most critical physical assets require the most stringent physical access controls). But in other cases, the reverse was true, with corporate office sites enforcing badge access while regional sites rely on manual processes, regardless of asset location.

At a minimum, organisations should implement the principle of least privileged access, whereby physical access permissions are aligned to role. This requires organisations to assess and prioritise the criticality of their physical sites, understand who is working at those sites, and align risk-based controls. (Note that this is a requirement for critical infrastructure operators under the revised SOCI legislation.) Risk based physical access controls may include badge access, biometrics, CCTV cameras, and the presence of security guards.

As organisations increase the maturity of their physical access controls, it is worth considering proactive monitoring of physical access data. Using behavioural analytic tools, organisations may consider baselining individual or peer group patterns of behaviour and responding to anomalies.

Virtual access management

Does your organisation 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?



Similar to physical access controls, all responding organisations noted some level of **virtual access management**. Vulnerabilities associated with virtual access management commonly arise from underlying systems issues including complex legacy systems. Unfortunately, it is common for large organisations, especially those that have grown through acquisition, to house personnel records in multiple systems. This makes it especially challenging to align and enforce access policies across an organisation. Furthermore, there is a high correlation between disaggregated data environments and access control failures such as accumulation of unnecessary access or lagging access following separation.

To effectively safeguard information and assets, organisations should employ the following core access controls:

> There are controls in place, but we need to improve. Access management uplift is part of the roadmap for our organisation. We're exploring the 'zero trust' framework.

> The only weakness that comes to mind is when people move roles. We don't give enough attention to what they do or do not need access to moving forward.

Centralised access management

Implement an identity and access management tool, linked to a single source of truth for user information (e.g. Active Directory), to enforce access policies in a consistent and organised manner.

Least privileged access

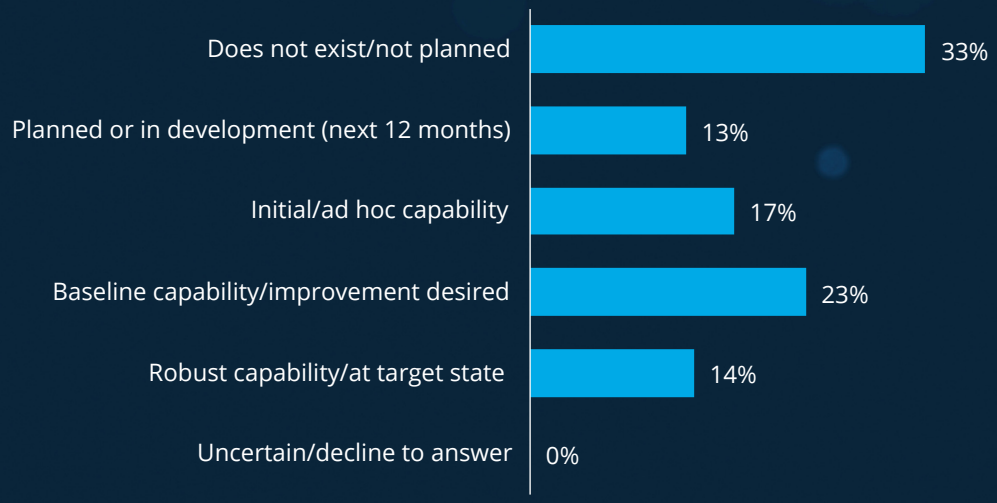
Align access permissions to job duties ensuring that sensitive information and virtual assets are only available to staff that require access. Supplement this with separation of duties protocols for critical IT actions.

Access reviews and visibility

Review accumulated privileges over time and reset accesses as required. Monitor users with policy exceptions and log unusual access requests. Ensure accesses are removed at the time of separation.

User behaviour analytics

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



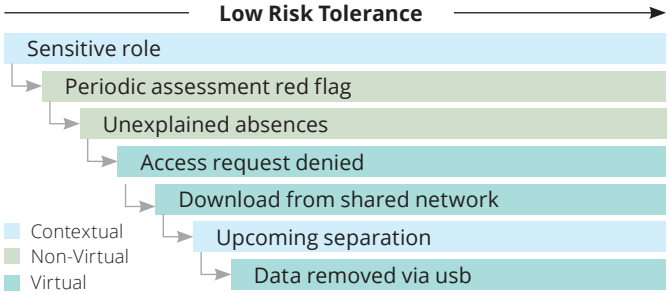
> It exists, but is limited. In our very unionised environment, we've been accused of spying. We need it, but the chance of getting it is low.

> Most of our analytics is reactive. There have been instances where we have picked up indicators showing an individual should be investigated further, but these are few and far between. There is a strong desire to improve here, but no specific plans in place. We're still assessing where it fits in the priority and resourcing matrix.

Many survey respondents discussed a desire to integrate physical and cyber security capabilities to view insider threat through a holistic lens. Deployment of a **user behaviour analytics (UBA)** solution is a key step in this integration and a foundational element of a mature insider threat program.

UBA is a capability that aggregates, correlates, and visualises **potential risk indicators (PRIs)** from across an organisation. PRIs represent behaviours in the form of actions, events, or conditions that typically precede an insider threat act. Optimised UBAs correlate both virtual and non-virtual PRIs from systems including DLP tools, IAM tools, personnel management, and human resources to proactively prioritise employee risk, as illustrated below.

Common PRIs

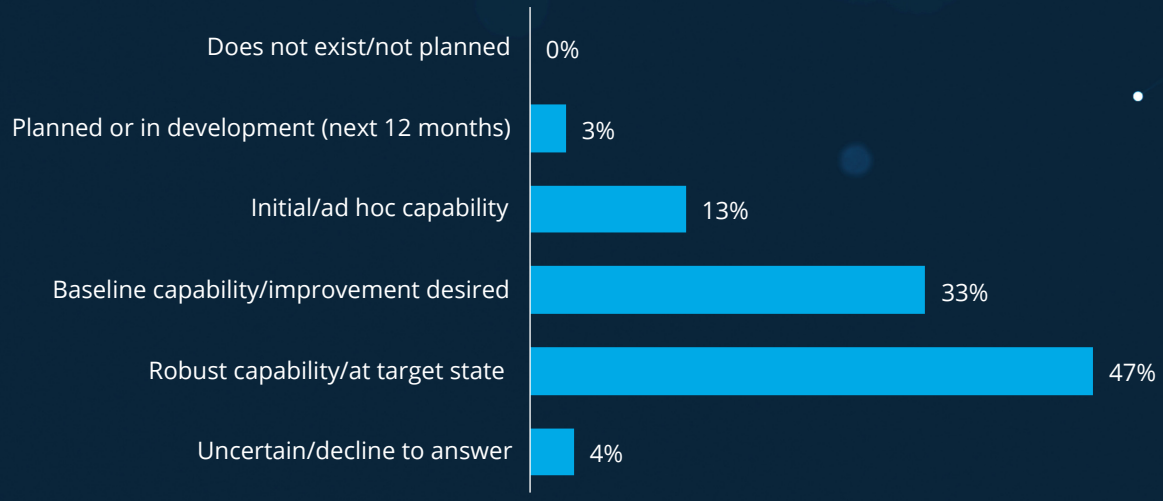


Key UBA set-up considerations

- Define PRIs through use cases that align to critical assets, prioritised threats and risk tolerance
- Leverage your working group to discuss data ownership and legal/privacy concerns
- Work with vendors or development teams to include privacy controls such as masking of monitored populations and auditing of investigations
- Develop escalation and triage plans that integrate with existing incident response plans

Insider threat incident response

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



> A cyber incident response plan is in place. The plan has a specific insider threat module – a playbook for insider threat data breaches.

> The process is good, the stakeholders are aware, and we know what to do. We're improving by adding new use cases nearly every week to build out the casebook.

Incident response is, on average, the most mature control type in Australia according to participating organisations. Many respondents have established investigations and incident response teams that have been responding to personnel security matters for some time. For some organisations, this includes robust documentation outlining the responsibilities of response stakeholders (including interactions with external regulatory and law enforcement bodies) as well as the use of case management systems to coordinate response actions over time.

As discussed on the previously, however, use of proactive detection tools is still limited. For those that do utilise detection analytics, there is a significant opportunity to improve the escalation and triage processes associated with managing proactive alerts and high-risk personas. This may necessitate the development of new response/referral pathways to promote employee support (e.g. use of employee assistance programs).

Ultimately, the goal of detection analytics is to focus the efforts of investigators towards risky behaviour within the organisation and to correct that behaviour before it results in damage. Integrating analytics-based escalation and triage pathways with traditional incident response plans will promote efficiency, enable agile collaboration, and move the organisation toward a more proactive mitigation posture.

Conclusion

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

Prevention posture

2.7/5

Readiness to prevent insider threats

Detection posture

2.9/5

Readiness to detect insider threats

Response posture

3.7/5

Readiness to respond to insider threats

As demonstrated throughout the control specific questions, most responding organisations have a baseline level of prevention, detection, and response controls in place. That said, many participants acknowledged that insider incidents, especially data exfiltration and fraud, are still likely to occur. Mitigating capabilities tend to be distributed across different functions and often narrowly applied resulting in gaps. Participants stated a desire to do more – to plug these gaps and minimise incidents that currently fall through the cracks.

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

Proactive posture

2.8/5

Most participants also noted some level of proactivity in dealing with insider threats. This included working to stem the tide of ignorant insider incidents through training and awareness programs, addressing insider risk through pre-hire screening, and proactively monitoring targeted virtual behaviours. The vast majority of respondents, however, noted that proactive efforts are narrow and ad hoc. Few organisations proactively address insider risk across their employee populations by understanding changes to individual risk profiles over time and intervening to correct concerning behaviour.

Effectively mitigating insider threats requires a comprehensive and risk-based program that is considered a shared responsibility among a cross-functional set of stakeholders. In today's complex working environment, mitigating controls must become smarter and more proactively employed. To operate most efficiently, control posture should align to prioritised assets, organisational risk tolerance, and risk assessments that are responsive to the evolving threat. Having too many security controls may impede your organisation's mission, yet having too few will leave the organisation exposed. Insider threat programs must strike a balance between countering the threat and accomplishing the organisation's mission. Quick responses, real-time data feeds, and proactive analysis of behavioural indicators are imperative to stay in front of the insider's exploitative tactics. The goal is to focus investigative resources on areas of greatest risk, detect anomalies as early as possible and interrupt the forward motion of potential insider threats before assets, data or personnel are compromised.

Appendix A: Guidance and regulation

There is a range of legislation and guidance related to insider threats. Some of these sources provide industry-specific requirements , while others provide industry-agnostic guidance. The below sources are a sample of the most relevant pieces of guidance and legislation for the Australian landscape.

The Australian Government's Protective Security Policy Framework (PSPF) and Information Security Manual (ISM)

Applies to: Australian Government entities

The Commonwealth PSPF outlines 16 security policies, including requirements associated with security governance, employee vetting, ongoing personnel suitability assessments, information access controls, and employee separation controls. The ISM provides coverage of malicious insiders, particularly in relation to data exfiltration, technical controls, and suppliers.

Security of Critical Infrastructure (SOCI) Legislation

Applies to: Owners and operators of Australia's critical infrastructure (11 sectors as defined by the legislation)

Extensive security legislation that requires critical infrastructure operators to address personnel hazard requirements within a written risk management program. This includes identifying critical workers, assessing the suitability of critical workers (i.e. vetting) and addressing risk arising from malicious/ negligent and separating employees and contractors.

Corporations Act 2001

Applies to: All public and private companies

Extensive regulation on businesses across Australia, which includes good faith provisions for officers and employees of a business (insiders) regarding the use of position and information. This relates to bribery and corruption, conflicts of interest, insider trading, and fraud and is regulated by multiple government entities including ASIC's Corporate Governance guidance.

Guidelines to counter foreign interference in the Australian university Sector

Applies to: Higher education institutions/universities

Guidance to increase resilience to the threat of foreign interference. This includes identification of key personnel (staff and students engaged in foreign collaboration) and use of information access controls.

Australian Government Personnel Security Handbook: Managing the insider threat to your business

Applies to: All Australian organisations

This Handbook provides general information, case studies, and high-level guidance to assist any Australian entity in understanding and mitigating insider threats.

Contacts

Jason Forsyth
Partner, Forensic
P: +61 2 9322 3307
E: jforsyth@deloitte.com.au

Paul Curwell
Principal, Forensic
P: +61 413 593 074
E: pcurwell@deloitte.com.au

Thomas Chandler
Director, Forensic
P: +61 426 642 665
E: thchandler@deloitte.com.au

Deloitte.