

Australian Government Insider Threat Program Guidelines

Release 2026

Contents

1. Introduction 3
2. Characteristics of an Effective Insider Threat Program 3
   - 2.1. Promotes a Positive, Robust and Supportive Workplace and Security Culture 4
     - 2.1.1. Understand Insider Threat 4
     - 2.1.2. Establish Reporting Mechanisms 4
     - 2.1.3. Engage with the Insider Threat Program 4
   - 2.2. Adapts as the Entity Evolves 5
   - 2.3. Implements Technology and Tools to Support the Insider Threat Program 5
     - 2.3.1. Policies to Support Technology and Tools 5
   - 2.4. Protects Sensitive Personal Information 6
3. Identification of Insider Risk and the Progression Towards an Insider Act 6
   - 3.1. Expressions of Insider Threats in the Workplace 6
     - 3.1.1. Espionage and Foreign Interference 6
     - 3.1.2. Sabotage 6
     - 3.1.3. Fraud and Theft 7
     - 3.1.4. Violence 7
   - 3.2. Types of Insider Threats 7
     - 3.2.1. Intentional Insiders 8
     - 3.2.2. Unintentional Insiders 8
4. Critical Pathway to Insider Risk 8
5. Indicators of Insider Risk 9
6. Commission of the Insider Act 9
7. Core Principles of an Insider Threat Program 10
   - 7.1. Principle 1: Develop an Insider Threat Program Framework 10
   - 7.2. Principle 2: Consider Legal and Privacy Rights 10
   - 7.3. Principle 3: Establish a Centralised Threat Analysis and Response Capability 10
   - 7.4. Principle 4: Identify and Incorporate Stakeholders 11
   - 7.5. Principle 5: Develop a Case Management Strategy 11
     - 7.5.1. Case Management Groups 12
     - 7.5.2. Group Membership and Meeting Frequency 12
     - 7.5.3. Implementing Case Management Strategies 12
   - 7.6. Principle 6: Define Accessible Paths to Information Required to Support the Insider Risk 12
   - 7.7. Principle 7: Safeguard Insider Threat Program Information 13
   - 7.8. Principle 8: Develop Process to Identify and Analyse Insider Risk Concerns 13
   - 7.9. Principle 9: Implement an Incident Response Plan for Insider Events. 14
   - 7.10. Principle 10: Deliver Insider Threat Awareness Training 15
8. Conclusion 15

1. Introduction

All Australian Government entities are vulnerable to insider threats, regardless of their size, function or risk profile. An insider threat program enables an entity to identify and manage insider risk in a holistic and coordinated manner. Under the Protective Security Policy Framework (PSPF), all entities are required to implement an insider threat program to manage the risk of insider threats in the entity.

Requirement 0051 | RISK | All entities | 31 October 2024

An insider threat program is implemented by entities that manage Baseline to Positive Vetting security clearance subjects, to manage the risk of insider threat in the entity.

This document has been prepared by the Department of Home Affairs, in collaboration with the Office of National Intelligence (ONI), and provides entities with a set of principles and guidance to assist them in building their insider threat program. The principles are based on current best practice and should be adopted by entities when developing their programs.

Further guidance at the PROTECTED classification is available by request from the Department of Home Affairs or the Office of the National Intelligence.

FOI: This is an exempt document under the *Freedom of Information Act 1982*. It must be handled in accordance with the *Office of National Intelligence Act 2018* and the PSPF.

2. Characteristics of an Effective Insider Threat Program

An insider threat program will need to make use of processes and systems that limit, control and monitor access within the entity. To support this, the insider threat program should have a strong framework and documented practices and be supported by a robust communications strategy.

Insider threat programs should:

- be tailored to the entity's unique mission, culture, critical assets, risk appetite and threat landscape
- be included in the entity's security risk assessment (SRA) and security risk management plan (SRMP)
- establish a positive security culture that supports the identification of risk and encourages reporting
- use a multidisciplinary approach that considers the entity's type, size, culture and risk tolerance levels
- include an approach that helps detect, identify, assess and manage the entire range of insider risks
- be supported by the entity's senior leadership team, and
- be enabled by process, policy and law.

A mature insider threat program will enable the entity to detect and identify concerning behaviours, assess and manage insider risks, and limit the consequences of insider events.

A well developed and successful insider threat program is one that:

- promotes a positive, robust and supportive workplace and security culture
- remains adaptable as the entity evolves
- implements technology and tools to support the activities of the insider threat program, and
- ensures the ongoing protection of sensitive personal information.

2.1. Promotes a Positive, Robust and Supportive Workplace and Security Culture

A strong foundation for insider threat prevention and detection is a positive, robust and supportive workplace and security culture. When this exists, staff will feel more confident to talk about concerns.

Developing and communicating the entity's expectations to its staff is an important part of creating and sustaining a positive workplace and security culture. Entities should:

- define the behaviours that are expected of all personnel, both inside and outside of the workplace, to protect the security classified information and resources that they have access to
- understand that expected behaviours will differ depending on the individual's role and location within the entity, and
- set security behaviours that the entity expects from third-party providers, vendors, contractors and visitors when they are engaged (physically or virtually) by the entity.

2.1.1. Understand Insider Threat

Delivering security awareness training and using promotional materials will help entities educate their workforce about insider threat. Security training and messaging will ensure that staff are well-informed about the risks, including personal vulnerabilities, as well as their security obligations.

PSPF Requirement 0024 mandates that all personnel (including contractors) receive security awareness training at engagement and annually thereafter. This obligations includes providing personnel with sufficient information and training on their protective security responsibilities

See PSPF Release 2026 (Section 3.5) and PSPF Guidelines (Section 3.5) for PSPF Requirements and guidance on security awareness training.

2.1.2. Establish Reporting Mechanisms

A key element of an insider threat program is to establish a clearly defined reporting mechanism and points-of-contact for reporting concerns that are easily accessible for all personnel.

PSPF Guidelines notes that effective security awareness training is most effective when, amongst other things, it clearly communicates to all personnel, including contractors, the entity's protective security practices and procedures. Security awareness training should therefore include advice to personnel on how to report any security concerns, and any actual or suspected insider threat activities. Training materials should also cover how the entity manages personnel security risks, including any confidentiality provisions and supporting mechanisms. This material should reinforce the expectation that, in accordance with PSPF principle 1, security is everyone's responsibility.

Entities need to build trust in the insider threat program. Personnel should know that any information they provide to the program will be kept in the strictest confidence.

2.1.3. Engage with the Insider Threat Program

The entity's insider threat program requires continued support and participation from all personnel, including senior leaders. The cultural, operational and financial benefits of the insider threat program should be communicated to the workforce to achieve and maintain support for the program.

The insider threat program should develop relationships with key senior leaders to act as 'champions' of the program.

2.2. Adapts as the Entity Evolves

Insider threats evolve on a continuous basis. An entity's insider threat program must be agile, resilient and adaptable to changes in the entity and the broader operating environment. The insider threat program should:

- adapt as the entity evolves and risk tolerance levels change
- improve based on best practice guidance and lessons learned from the broader insider threat community (including other Australian Government entities and international partners), and
- implement an ongoing program to review entity risks, ensuring a current and accurate risk picture.

The program also requires ongoing sustainment and resource allocation to commensurately match the entity's evolution.

2.3. Implements Technology and Tools to Support the Insider Threat Program

There are a variety of technologies and tools available to help entities identify insider threats. These should be used in conjunction with non-technical data sources to inform the insider threat program. The use of any technical capability should be supported by the entity's insider threat team, other internal stakeholders and senior managers.

When entities are looking into technologies and tools that will be used to support their insider threat program, they should look to ones that will collect the following types of data:

- Alerts – real time notification that show a specific, pre-configured event has occurred
- Content – data held within a data payload intended for communication, transport or processing
- Flows – network metadata that describes the transport of data across a Transmission Control Protocol/Internet Protocol (TCP/IP) network but does not contain the information being communicated
- Logs – records of events that have occurred within a device, system or application, and
- Identity – data that may contain characteristics that describe a specific individual.

When looking at purchasing technologies or tools entities should consider:

- their ability to limit access (role-based access)
- their ability to import/export information, and
- the overall lifecycle cost and resourcing impost.

Any tools that are used by the entity should be configured to meet their specific requirements. Consideration should be given to the entity's profile, critical assets and risk tolerance, and configurations should complement the human element of the insider threat program. Technical tools and systems should be reviewed regularly.

2.3.1. Policies to Support Technology and Tools

Entities should have policies in place to support activities that are undertaken by any insider threat technologies and tools used by the entity. Policies should:

- clearly articulate the scope of use for the technologies and tools
- ensure compliance with relevant legislation and policies, including the PSPF
- ensure compliance with privacy requirements, and

- describe information sharing arrangements between cyber security areas and the insider threat program.

See ASD's Information Security Manual (ISM) for further guidance on the use of cyber security monitoring

2.4. Protects Sensitive Personal Information

Personnel involved in managing the entity's insider threat program will have ongoing access to sensitive information about entity personnel and their behaviour. The insider threat program must find a balance between the protection of personnel privacy and the protection of the entity against insider threats.

For the insider threat team to effectively undertake their role, the entity should and appoint the right people to undertake this sensitive work and consider the security clearance level required for team members to work in the insider threat team.

3. Identification of Insider Risk and the Progression Towards an Insider Act

Insider risks can be observed in the workplace, enabling their detection and identification. Entities should establish methods of detecting and identifying actual or potential insider acts, including individuals demonstrating concerning behaviours or changes in their personal circumstances.

Entities should equip supervisors to use the annual security check (mandated in PSPF Requirement 0168) as an additional means of tracking insider risks or security concerns. Insider risks can also be identified through information shared through vetting processes.

3.1. Expressions of Insider Threats in the Workplace

Insider acts can manifest in the workplace in a number of different ways.

3.1.1. Espionage and Foreign Interference

Espionage is the theft of information by someone either acting on behalf of a foreign power or intending to provide information to a foreign power which is seeking advantage over Australia. Espionage can target Defence, political, industrial, foreign relations, commercial, or other information that is usually otherwise unavailable to the foreign power.

Foreign interference involves covertly shaping decision-making to the advantage of a foreign power and is hostile to Australia's interests. It is not the same as a foreign state taking open and transparent action to influence deliberations of importance to them. Interference is activity that is done in secret by (or for) a foreign actor which is deceptive, corrupting or threatening in nature and contrary to Australia's sovereignty and interests.[1]

3.1.2. Sabotage

Sabotage is the deliberate action of a trusted insider aimed at harming an entity's infrastructure. This can include facilities, equipment, infrastructure or information and communication technology (ICT). It can be conducted both physically and virtually and is not limited to irreversible and destructive attacks – small scale, selective and temporary acts of degradation or disruption are also defined as sabotage.

[1] ASIO, '*Counter-espionage and foreign interference*', http://www.asio.gov.au/about/what-we-do/counter-espionagewww.asio.gov.au/about/what-we-do/counter-espionage, accessed 27 September 2024.

ICT sabotage is typically committed by technical users with privileged access, such as system administrators, database administrators, and programmers. A common motivation for ICT sabotage is revenge for a negative workplace event. An employee may set up a malicious action while still employed but defers execution to a future time, usually following termination of employment.

3.1.3. Fraud and Theft

Fraud is defined as dishonestly obtaining – or attempting to obtain – a benefit, or causing a loss or risk of loss by deception or other means.[2] Personnel may be motivated to commit fraud to gain a benefit for themselves or others, or to cause a loss to the entity or the government. The dishonest benefit gained or loss caused by fraud is not just limited to a monetary cost (e.g. theft). It also includes information, intellectual property (IP) and time (e.g. personnel fraudulently manipulating leave).

Fraud can be committed by an individual to benefit themselves or on behalf of an external agent. It can also be committed by a network of individuals conspiring together. Fraud can be facilitated by unwitting co-workers who are unaware they are helping a fraudulent individual.

Theft of IP can be committed by entity personnel with access to specialised or classified IP, such as scientists, engineers, researchers, project managers, programmers and contracted personnel. These personnel may steal the information they worked on and take it with them as they leave the entity to start their own business, start a new job, or to disclose to a foreign government or organisation.

3.1.4. Violence

Violence from an insider threat is defined as any act of violence, threat of violence, or other threatening behaviour that creates an intimidating, hostile, or abusive environment. Workplace violence occurs in the workplace or while personnel are working, wherever that may be. Examples of workplace violence include:

- physical violence (including terrorism)
- harassment (including sexual harassment)
- intimidation
- bullying, or
- jokes or comments that cause offence or distress.

3.2. Types of Insider Threats

All current or former employees or contractors who have legitimate or indirect access to a workplace's people, information, techniques, technology, assets or facilities are defined as trusted insiders (insiders).[3] The insider threat is when a trusted insider intentionally or unintentionally uses their access to conduct activities that could cause harm or negatively affect a workplace. These insiders are referred to as intentional insiders and unintentional insiders, respectively.

Insider activity can damage an entity's reputation, be highly disruptive to operations and – in the worst-case scenario – be life threatening. While there are a diverse range of motivations behind the actions of intentional and unintentional insiders, both place personal motivations and needs ahead of their obligations to their entity – including colleagues, workplace, government and country.

[2] Attorney-General's Department, *Commonwealth Fraud and Corruption Control Framework 2024*, p.41.
[3] ASIO, Managing Insider Threat: A Security Managers Guide, p.2 and p.5.

3.2.1. Intentional Insiders

Intentional insiders are individuals who deliberately or knowingly betray the trust placed in them.

3.2.2. Unintentional Insiders

Unintentional insiders are individuals who inadvertently or unknowingly betray the trust placed in them.

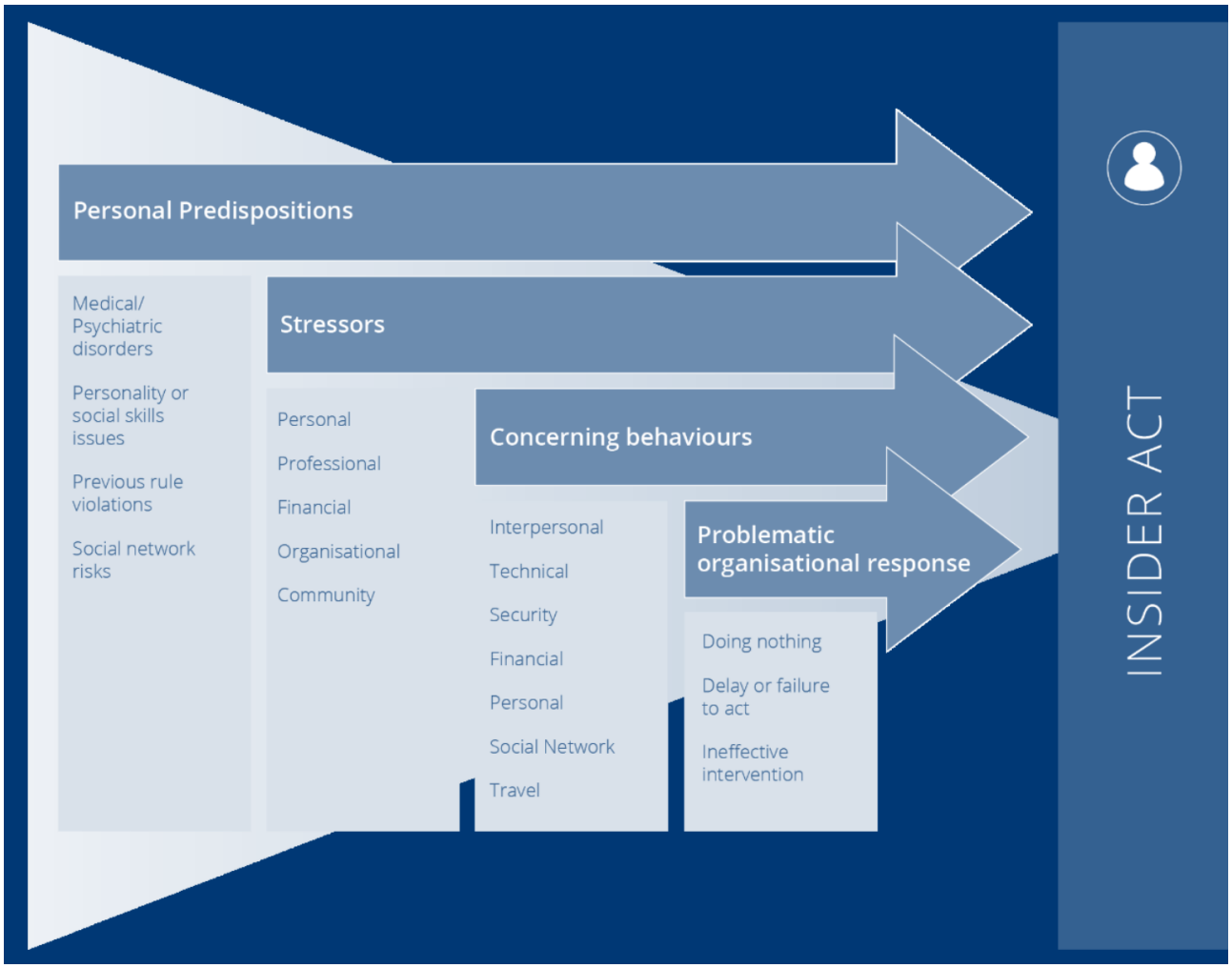
The potential harm of insider activity can be significant, regardless of whether an act is intentional or unintentional. However, unintentional insider threats can be more difficult to anticipate due to their basis in potential negligence, carelessness, ignorance or 'human error.'

Note: both intentional and unintentional insiders may help a third party, such as a foreign power or their proxy. They may willingly assist, be coerced to assist, be unknowingly exploited, or be unaware their actions are harmful.

4. Critical Pathway to Insider Risk

While all people experience stressful events, the majority will do so without resorting to disruptive or destructive acts in their personal lives or within the workplace. For those who do turn to intentional malicious activity, researchers have determined that these acts are rarely spontaneous, and are usually the result of a deliberate decision to act.

Figure 1: Critical Pathway to Insider Risk



Shaw and Sellers describe the evolution from trusted insider to insider threat as the Critical Pathway to Insider Risk.[4] This framework demonstrates how an individual's personal predispositions and stressors can result in observable behaviours of concern, and how an entity's response – or lack thereof – can progress an employee towards undertaking an insider act (see Figure 1 Critical Pathway to Insider Risk).

Progression along the Critical Pathway can be fast or slow depending on the individual's circumstances. Warning signs, stressors and concerning behaviours are often evident before an insider event occurs and can be seen at any stage on the pathway. Once a trusted insider begins moving along the pathway, they are more likely to act. When an entity detects concerning behaviour but does not take appropriate action, they could increase the likelihood of an insider act occurring. Special attention should also be given to individuals who resign suddenly or have their employment terminated.

5. Indicators of Insider Risk

Indicators of insider risk relate to an individual's behaviours, stressors, personal predispositions and background that may indicate an increased likelihood of committing an insider act. These indicators can help flag an individual for additional consideration, monitoring or assessment.

There are a large number of indicators and they broadly fall under the following categories:

- personal
- behavioural
- technical, and
- organisational

Additional information on indicators can be found in the PROTECTED version of this guidance which is available on request from Department of Home Affairs.

6. Commission of the Insider Act

Once an individual decides to act maliciously, evidence of their progression towards the final act can be observed through their behaviour. This progression is outlined in Figure 2.

- Grievance and ideation – the expression of an individual's distress, reason for disgruntlement or resentment. It could also be a personal, professional or entity stressor. Whatever the reason, it is the beginning of an individual's progression from their initial idea to action.
- Preparation – the individual's grievance will manifest into observable planning behaviours. This can include conducting research, developing a plan and acquiring items or accesses that will be needed.
- Exploration – the individual will commit to undertaking an insider act. This could be due to an additional stressor including an unhelpful entity response. During this stage the individual will begin to seek weaknesses in security, find new access points, decide what data or asset they want to destroy, misuse or steal, and may solicit help from others.
- Experimentation – individuals will review and refine their plan. They may begin to undertake surveillance of certain locations, attempt access to the required facility or ICT system, appear in areas where they don't belong or start to test the entity's boundaries.

[4] E Shaw and L Sellers, *Application of the Critical-Path Method to Evaluate Insider Risks* (2015) 59:2, Studies in Intelligence, pp1-8.

- Execution – with the hostile attack formulated, planned out and rehearsed, the individual will take advantage of their access and knowledge to execute their plan.
- Escape – individuals will often develop an escape strategy before conducting the insider act. This could include shifting blame, altering records and covering movements or malicious actions.

Figure 2: Intentional Insider Act Progression



7. Core Principles of an Insider Threat Program

The core principles of an insider threat program provide a structured framework for entities as they design and implement their insider threat program. A program designed in accordance with these principles will enable proactive identification and management of insider threats.

7.1. Principle 1: Develop an Insider Threat Program Framework

An insider threat program is a high-level document that establishes governance arrangements, objectives and stakeholders of the program. It promotes entity-wide participation, a common vision, defines the goals of the program, and describes the current threat environment. The program framework is supported by policies, plans and processes that formalise the program's activities.

The insider threat framework should be formally endorsed by a relevant delegate within the entity.

7.2. Principle 2: Consider Legal and Privacy Rights

Insider threat programs draw on sensitive personal information about an entity's personnel. The actions and decisions of the insider threat program have the potential to significantly – and adversely – impact an individual's career and reputation. As such, the insider threat program must comply with all relevant legislation and policies. Program activities must follow due process and adhere to the principles of procedural fairness. Insider threat program stakeholders must adhere to the need-to-know principle to preserve the privacy of individuals involved.

7.3. Principle 3: Establish a Centralised Threat Analysis and Response Capability

Insider threat programs require entity-wide coordination and collaboration from key stakeholder areas – such as security, human resources and legal. However, best practice guidance recommends a centralised insider threat management team should coordinate the program, drawing on relevant stakeholders when necessary.[5]

As such, entities should have a centralised capability for insider threat analysis and response. This capability will have responsibility for the day to day running of the program and play a key role in the identification, analysis, prioritisation and management of insider threat concerns identified within the entity.

[5] ASIO, *Countering the insider threat: a security manager's guide*, p.19; Carnegie Mellon University Software Engineering Institute (SEI), *Common sense guide to mitigating insider threats* (7th edition), p.23.

7.4. Principle 4: Identify and Incorporate Stakeholders

Insider threat programs require entity-wide coordination and collaboration. Sponsoring Entities should establish formal arrangements to ensure the information maintained by stakeholders is regularly fed into the insider threat program promptly and securely.

Building positive working relationships with stakeholders and educating them about the purpose of the insider threat program is an effective way to secure buy-in from areas that may not be familiar with insider risk management or the role that they play within the insider threat program.

If stakeholders understand the intent of the program and their role within it, they are more likely to collaborate.

Stakeholders who should be incorporated into insider threat programs are listed below:

- senior leadership
- insider threat team
- human resources
- cyber security
- physical security, and
- legal.

Some stakeholders may not be permanent members of the program. For example, depending on the entity, legal may only be required to engage on an as required basis. This may include when the entity initially establishes insider threat policies and procedures – to ensure compliance with legislative frameworks – and subsequently when undertaking administrative action such as employee suspension or termination.

In addition to the above internal stakeholders, entities should routinely engage and communicate with the external stakeholders below:

- the relevant Authorised Vetting Agency, and
- the Department of Home Affairs.

7.5. Principle 5: Develop a Case Management Strategy to Manage Current and Emerging Insider Risk Concerns/Issues

Effectively managing insider threats can stop an individual of concern moving along the Critical Pathway to Insider Risk and reduce the likelihood of an insider act occurring. Implementing sound processes and collaborating with key internal stakeholders enables an entity to influence an insider's trajectory along the Critical Pathway. These processes are generally referred to as case management and are the way that identified insider threat concerns are managed on an ongoing basis.

Entities should invest in planning and establishing case-management processes, ensuring they are tailored to the size and requirements of the entity. Depending on the nature of the insider risk and the significance of the concern, case-management processes may involve different stakeholders and require different levels of seniority. If appropriate, entities can leverage existing enterprise risk management committee structures to meet their insider threat case management requirements. However, entities can also create new structures. A multi-tiered approach to managing insider risks ensures cases can be escalated for further scrutiny and senior decision making as required.

7.5.1. Case Management Groups

Proactive case management is an essential component of an insider threat program. A multi-tiered case management structure is recommended as best practice. This enables case management to occur at different levels and with appropriate stakeholders, depending on the significance and nature of the insider risk.

An entity's case management framework should be tailored to the size and requirements of the entity. In addition to routine case management processes, entities should implement a working level case management group and a senior level case management group wherever possible.

Case management groups are convened to support the identification, analysis and management of insider risk within the entities. The case management groups will generally be responsible for:

- escalating cases to a more senior committee when required
- determining next steps and management strategies
- formally recording meeting outcomes, decisions and actions, and
- implementing management strategies.

7.5.2. Group Membership and Meeting Frequency

All case management groups should include insider threat team members and representatives from other insider threat stakeholder groups as required. Both working level and senior level case management groups should be convened regularly to ensure entity responses to insider risk concerns are coordinated and informed by personnel security considerations.

Working in this collaborative fashion enables:

- knowledge sharing
- holistic management of identified risks
- quick response to emerging risks
- limiting problematic entity responses, and
- building a common approach to deterring, detecting, and managing insider risks.

7.5.3. Implementing Case Management Strategies

Case management strategies are actions that are carefully planned and implemented to manage the risk posed by individuals of concern. These may include overt or covert actions to obtain information, or direct interventions to manage risk. Entities should identify available case management strategies within their insider threat program framework.

Case management strategies should be planned and implemented on a case-by-case basis. The appropriate strategy will depend on the complexity of the case, the nature of the insider risk and the implications for the entity. Management strategies should be holistic and flexible, and entities should understand they may not work as planned.

7.6. Principle 6: Define Accessible Paths to Information Required to Support the Insider Risk

Both technical and non-technical data sources have an important role to play in any insider threat program. These sources feed vital information into the program and can help to proactively identify concerning

behaviours in the workplace. Entities should determine the best way to feed this information into their insider threat program.

Information sources can include:

- human resources
- physical and information security
- personnel security, and
- cyber security

The insider threat management team will also need to share information with identified stakeholders. Information sharing agreements should be formalised if they are required.

7.7. Principle 7: Safeguard Insider Threat Program Information

The information accessed and used by the insider threat program is sensitive and needs to be protected. The following examples of protection strategies can be considered when developing an entity's insider threat program:

- all information is classified, stored and handled in accordance with the PSPF and any other relevant policies and procedures
- access to information is determined on a strict need-to-know basis
- where possible (or required under the PSPF), program information is encrypted when it is sent by email, and
- distribution lists are restricted to essential personnel only.

Entities should consider storing insider threat program data in a central information repository, which serves as a 'single source of truth' for the insider threat program.

A central information repository should support:

- information access controls
- the ability to store and manage a variety of information types, and
- the ability to store large amounts of data.

It is important to consider storage, archiving and access requirements for any repository that is used or developed.

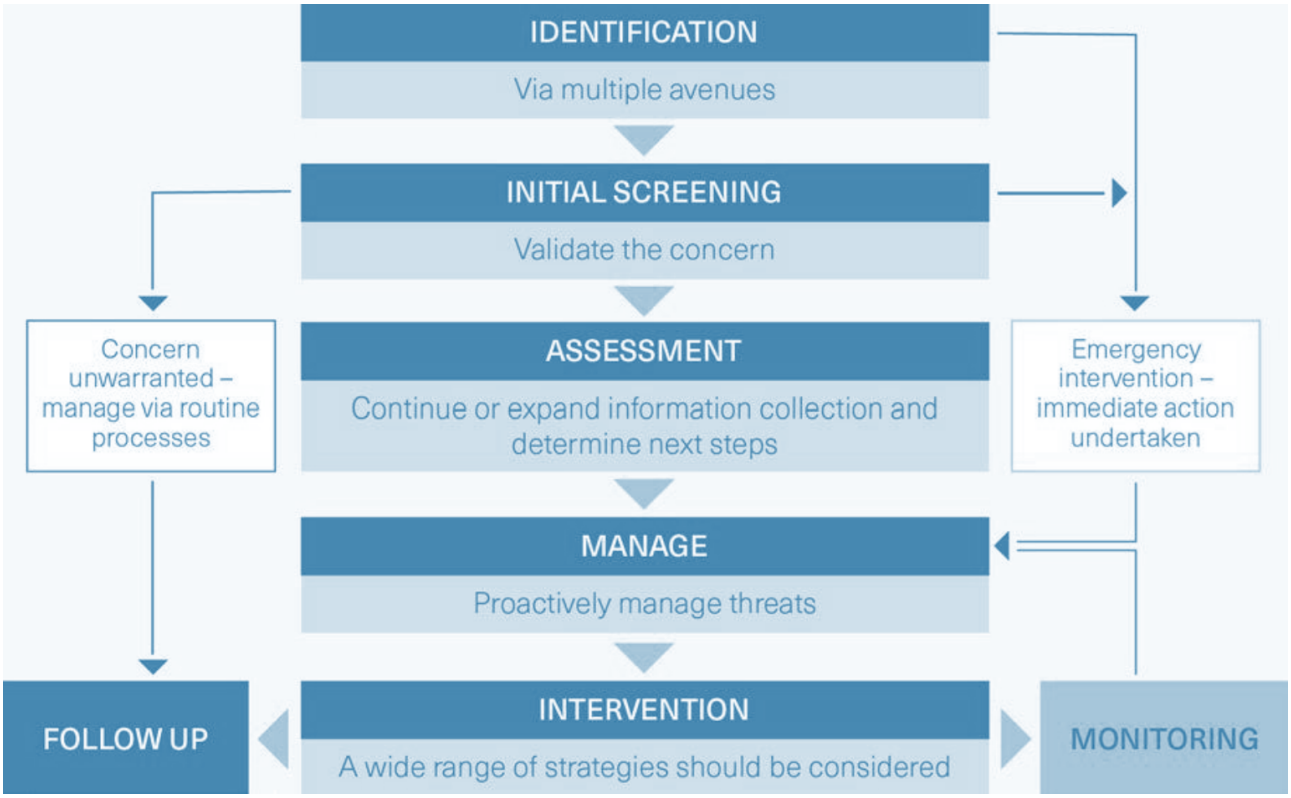
7.8. Principle 8: Develop Process to Identify and Analyse Insider Risk Concerns

There are many ways the insider threat team will become aware of concerns. Entities should:

- enable confidential reporting and ensure confidentiality is maintained in any subsequent activities
- develop multiple reporting avenues, including online, phone and face-to-face options, to improve the availability and accessibility of reporting, and
- acknowledge reports to the insider threat program promptly so personnel know that all reports are considered and taken seriously.

Entities should plan and formally document the insider risk assessment process. Entities can use the following process outlined in Figure 3 as a guide.

Figure 3: Suggested Insider Risk Assessment Process



Insider risk assessment involves compiling and analysing information about an individual where concerns have been raised with the insider threat team. When developing an assessment process, entities should consider the scope of the insider threat program, what data collection tools are available and the maturity of their program.

Consider the following assessment questions:

- Is there evidence to suggest the individual of concern poses a threat?
- What type of threat does the individual of concern pose?
- Is the individual of concern progressing along the Critical Pathway to committing an insider act?

7.9. Principle 9: Implement an Incident Response Plan for Insider Events.

PSPF Requirement 0026 mandates that procedures are developed, implemented and maintained to ensure security incidents are managed and responded to. While there are similarities between other security incidents and insider events, they are each distinct and require specific response planning to manage.

An insider event response plan describes the processes, procedures and principles of an entity's response to an insider event. Additional considerations for responding to insider events include:

- defining roles and responsibilities
- having clear processes for reporting and escalating insider events
- developing guidelines for communication and information sharing within the insider threat program, with insider threat program stakeholders, across the whole entity and externally
- developing processes to manage the inherent sensitivities associated with insider threat events
- ensuring that guidelines for engagement with relevant external agencies are in place.

7.10. Principle 10: Deliver Insider Threat Awareness Training

Highly aware and trained personnel play a key role in the early identification of insider threats.

Insider threat awareness training for all personnel should:

- define types of insider threats, describe potential motivations and behaviours associated with each type, and highlight the potential consequences of insider activity
- identify and describe entity-specific reporting processes and other employee obligations within the insider threat program, and
- use real-world case studies to reinforce key points.

Insider threat awareness training should form part of each entity's on boarding process for new staff. It should also be included within the entity's annual security awareness training package – either as a discrete and independent section of the training package or integrated within existing courses. Training compliance should be recorded, documented and tracked.

Entities should supplement formal training requirements with products that reinforce insider threat messaging. These could include:

- posters or electronic signage
- communication campaigns, such as blog posts or all staff emails, and
- handouts or leaflets.

8. Conclusion

The preceding guidance outlines the principles entities should consider when building their insider threat program. This guidance does not prevent entities that have access to unique information sources or advanced capability from implementing programs that build upon these principles.