Te Pā Whakamarumaru
New Zealand Security Intelligence Service

Secure your team

Five principles for managing insider risk

The New Zealand Security Intelligence Service (NZSIS) is responsible for leading the discovery, investigation, and assessment of insider threats within government.

When investigating potential insider threats, NZSIS prioritises activity considered higher harm to New Zealand's national security, such as:

- unauthorised disclosure of official information (whether it is classified, or not)
- theft or sabotage of New Zealand Government resources or assets that adversely affects national security
- behaviour indicative of espionage, loyalty to foreign interests, or support for violent ideologies.

We regularly collaborate with domestic and international partners to produce best practice advice for identifying insider threats and managing risks. The guidance is intended to be practical and be used by any organisation to prevent, mitigate, and respond to both actual and potential insider threats.

NZSIS assesses both public and private sector organisations in New Zealand are vulnerable to harm from insider threat activity.

Foreign states are increasingly targeting insiders for espionage opportunities by trying to convince or manipulate them to share protected information. It is known that criminal actors are a concern too along with those who inadvertently cause harm. NZSIS continues to see instances of deliberate, influenced, and unwitting insider acts.

Our *Secure your team* guidance is based on latest research and recent experience. It is designed to help organisations make their insider threat programmes more effective based on a clearer understanding of the issue and what causes it. Adopting the five principles will help create a workplace where security is seen as a shared responsibility and more effective interventions can happen.

Who is this guide for:

A robust security culture is best set at the top of an organisation. Chief executives and board members need to understand and ask questions on what security measures are in place and take responsibility for them.

Chief security officers, compliance officers, and human resources practitioners are encouraged to develop an insider threat programme that creates a shared understanding of the risks and what needs protecting. It needs to be tailored to your existing organisational culture and security settings.

Secure your team outlines five key principles that should form the basis of any insider threat programme.

Principle 1:
Adopt a shared language

NZSIS provides definitions to encourage consistency and highlight that both unintentional and intentional insider acts can cause harm to organisations.

Principle 2:
Broaden your understanding of potential insider threats

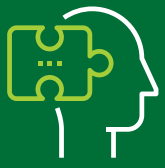
Understanding common types of insider acts and their impacts will help you to consider what assets need protecting and how they might be harmed.

Principle 3:
Consider the 'spectrum of intent' from unintentional to intentional insider activity

If you employ people, you have insider risk. Insider acts are more often unintentional than deliberate so consider developing a holistic programme that acknowledges a broad range of causes. Find ways to build staff engagement on the topic of security and adopt measures that support resilience.

Principle 4:
Detect signs of insider risk and act to de-escalate

Reviews of previous cases reveal a common set of observable behaviours and activities associated with insider risk. Learn the lessons of hindsight to identify opportunities to intervene early to manage risk early before it escalates.



Principle 5:
Learn the foundations for effective interventions

Consider what drives insider risk and the various potential mitigations. Develop an effective security culture and shape your workplace environment in a way that limits the opportunities for intentional or unintentional insider acts.

Principle 1
Adopt a shared language

Clear definitions that are used consistently across an organisation helps everyone to be on the same page.

The definitions provided are designed to help bring about a common understanding of key concepts related to insider risk.

A key point to remember is that if you have people, you have insider risk. Everyone who has access to your organisation or has previously had access can pose a risk. This can include people in your supply chain.

It is recommended you use the following definitions when assessing or managing insider risk to avoid confusion and misinterpretation.

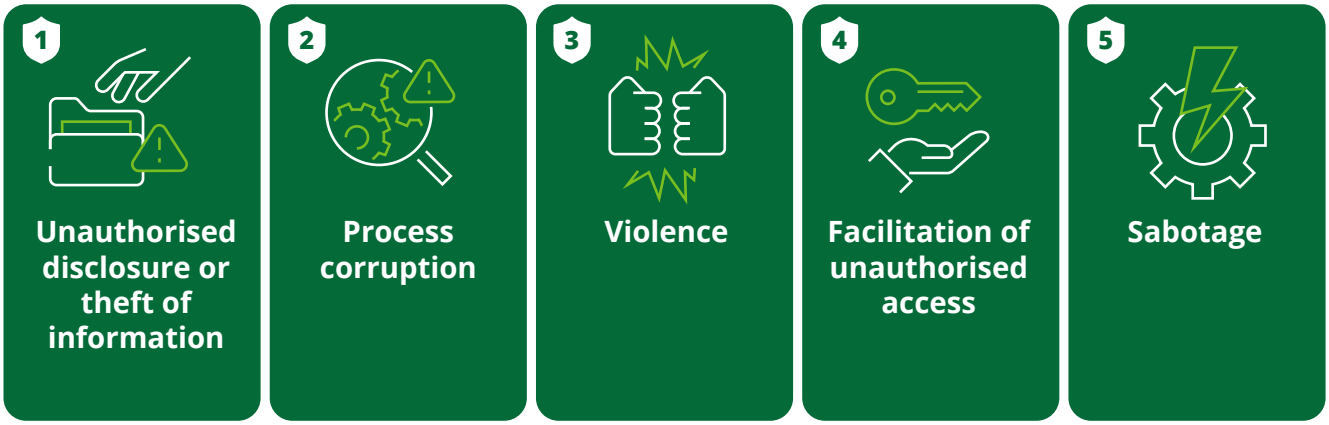
- **Insider** – Any person who has, or previously had, authorised access to or knowledge of the organisation's resources, including people, processes, information, technology, and facilities.
- **Insider Risk** – The likelihood of harm or loss to an organisation, and its subsequent impact, because of the action or inaction of an insider.
- **Insider Threat** – An insider, or group of insiders, that either intends to or is likely to cause harm or loss to the organisation.
- **Insider Act** – The activity, conducted by an insider (whether intentional or unintentional) that could result in, or has resulted in, harm or loss to the organisation.

Be creative when raising awareness about insider risk. Talk about security in a way that connects with your organisation's culture so your people have a strong understanding about why these threats are credible and the role team members can play to minimise risk.

Principle 2
Broaden your understanding of potential insider threats

Organisations can fall into a trap of adopting a perspective that is too narrow on what is considered an insider act and can miss the full range of ways an insider can cause harm.

Secure your team groups insider acts into five common categories noting that these are not exhaustive and will differ from sector to sector. Consider the critical assets your organisation will need to protect against the following categories of insider acts.



1. Unauthorised disclosure or theft of information

- **State espionage** – passing information that may provide an advantage to another government, state, or foreign intelligence service;
- **Corporate espionage** – unauthorised disclosure of Intellectual Property (IP) to another company or competitor;
- **Personal theft of IP** – taking IP for personal use, such as for future employment or to sell for personal gain;
- **Media disclosure** – giving information to a media organisation without authorisation.

2. Process corruption

- **Fraud** – intentional act involving deception to secure unfair or unlawful gain;
- **Criminal facilitation** – using an organisation's data to facilitate organised crime;
- **Abuse of powe**r – using official authority gained through the organisation for personal gain;
- **Malign influence** – use of subversive, deceptive, or coercive methods to manipulate attitudes, perceptions or behaviours to advance their interests or objectives.

3. Facilitation of unauthorised access

- **To a physical building or asset** – enabling unauthorised access to physical assets;
- **To IT systems** – enabling unauthorised access to corporate or restricted networks or systems;
- **To people** – enabling privileged access to people for the purpose of gaining unauthorised, inappropriate or potentially harmful influence.

4. Sabotage

- **Physical sabotage** – physically damaging assets;
- **Electronic sabotage** – reducing the availability, integrity or confidentiality of data on IT systems, deleting data on a server;
- **Reputation sabotage** – intentionally undermine reputation of an organisation by spreading false information.

5. Violence

- **Sexual or violent crime** – using privileged access to facilitate an attack against another person.
- **Terrorism** – using inside access to facilitate or carry out terrorism.

It is important to note that insider acts can feature multiple acts. For example, an insider may facilitate unauthorised access to support an act of sabotage or violence.

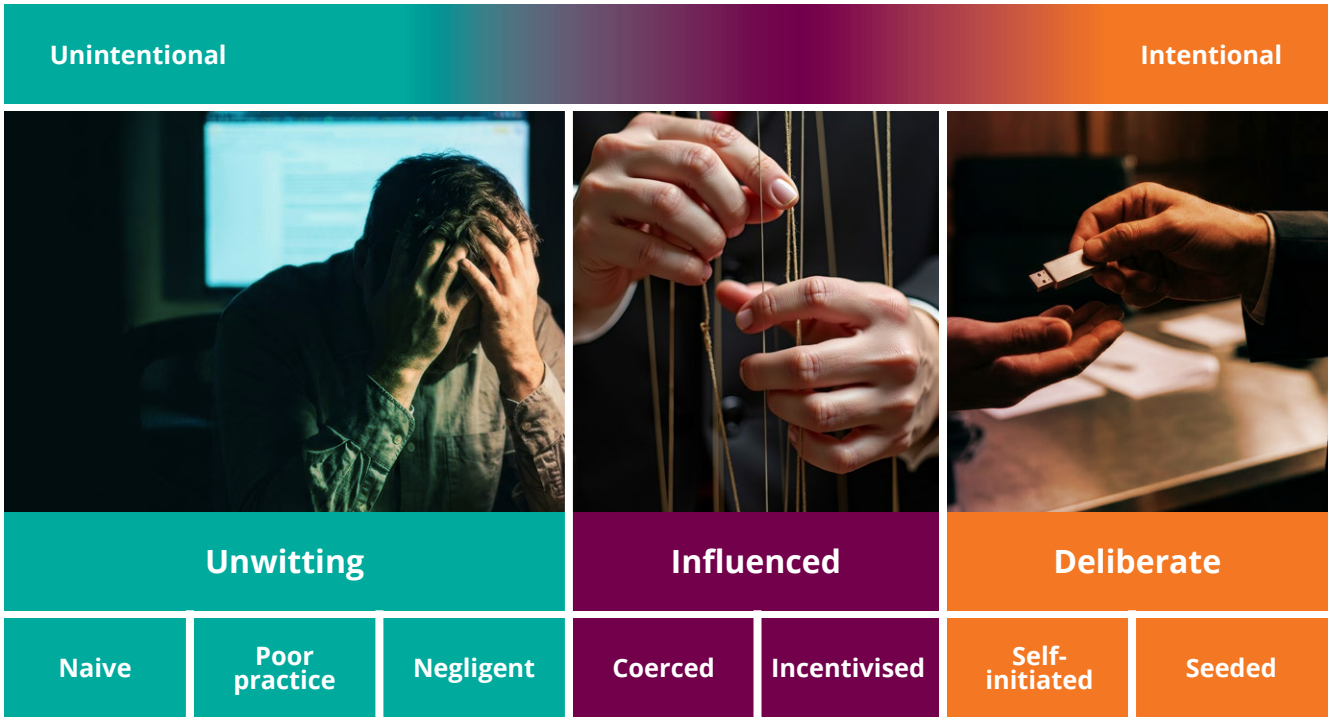
Use the Protective Security Threat and Risk Guidance to conduct simple security threat and risk assessments against these five categories to ensure you apply the appropriate amount of resource to areas of higher risk. See https://www.protectivesecurity.govt.nz/assets/psr/protective-security-threat-and-risk-guidance.pdf

Principle 3
Consider the 'spectrum of intent' from unintentional to intentional insider activity

Insider threat programmes in organisations have typically focused on reducing risk from intentional insiders but research shows unintentional insider acts also have a long-lasting and widespread impact.

A modern approach requires understanding that insider acts can be deliberate, influenced or unwitting and that different interventions are required to manage the risk effectively.

The spectrum of intent to cause harm



Unwitting

Unwitting insiders typically cause harm through their own naivety, poor practices or negligence. Their actions can expose security vulnerabilities in an organisation that could be exploited by others.

Naive insiders are victims of malicious actors and have been tricked or deceived.

Example: giving unauthorised access to someone with a fake pass.

Insiders with **poor practice** might unknowingly break the rules by failing to comply with security processes.

Example: Thinking they have secured a door but failing to follow proper process meant the lock did not engage and someone gained unauthorised access.

Negligent insiders knowingly break the rules, without setting out to harm the organisation.

Example: Emailing sensitive information to an insecure personal account, knowing this is against policy, just so they can complete a work task from home.

Influenced

Influenced insiders may be coerced or incentivised to cause harm. They might face external pressure from foreign states or criminal entities, or from individuals who wish to harm the New Zealand government or our national security.

Coerced insiders act from fear of negative consequences.

Example: someone may be motivated to act after being threatened that their family will be harmed.

Incentivised insiders act primarily for personal benefit.

Example: a person is paid in order to facilitate unauthorised access to an organisation's operating system.

Deliberate

Deliberate insiders knowingly seek to cause harm or loss to the organisation. There are two main types:

Self-initiated insiders join legitimately then use their access for unauthorised purposes.

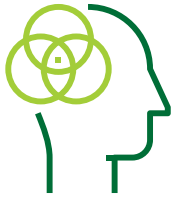
Example: leaking sensitive material with intent.

Seeded insiders join with the aim of exploiting their access to assets.

Example: a foreign state co-opts an insider to conduct espionage or they place an agent in in an organisation for the same purpose.

Improve the way you talk to your teams about security to reinforce that unwitting acts can also cause harm and colleagues can support each other to identify potential threats. Back this up with clear, confidential and non-punitive channels for employees to report concerns. Many organisations use the phrase 'see something, say something' but choose something that fits with the culture of your workplace.

Principle 4
Detect signs of insider risk and act to de-escalate



Insider threats never emerge without some kind of early warning.

Previous insider acts that have come to light have taught us that risk evolves over time. There will often be visible signs and potentially multiple chances to detect and disrupt insider threats. It is important to understand why and how someone who legitimately joins a workplace, without any intention of committing an insider act ends up causing harm to the organisation.

The critical pathway to insider risk framework helps to identify issues an employee could be facing and think about the opportunities to intervene early and prevent escalation.

Research[1] has identified four factors that can increase insider risk and how these might appear in the workplace.

1. **Personal predispositions**

   These are intrinsic traits or past experiences, such as personality disorders, lack of social skills, a history of rule violations, or risks associated with an employee's social networks outside of work that make an individual more susceptible. They represent the underlying vulnerabilities an employee brings into the organisation.

2. **Stressors**

   These are significant life events that trigger an individual's predispositions. Such pressures can push an employee further down the pathway toward potential malicious intent.

3. **Concerning behaviours**

   These are observable indicators in the workplace that signal an escalation of risk. Most insiders exhibit these smaller warning signs long before committing a serious act.

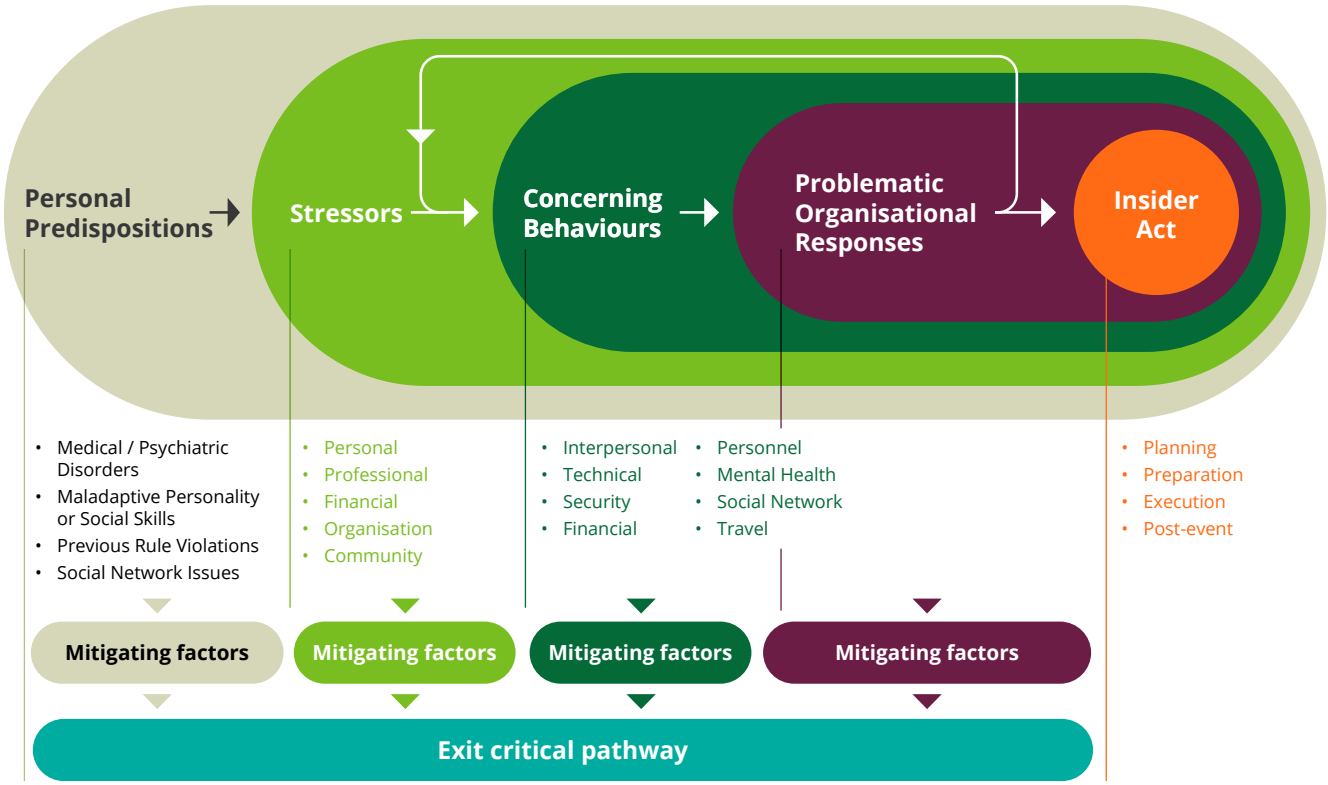
4. **Problematic organisational responses**

   When an organisation ignores warning signs or responds in a counterproductive way, it can further alienate the employee and solidify their trajectory toward a harmful act.

1 *E. Shaw and L. Sellars, Application of the Critical Path Method to Evaluate Insider Risk, Studies in Intelligence, vol.59, no.2, June 2015 & Shaw, E.D. (2023). The psychology of insider risk. CRC Press.*

The critical pathway to insider risk (adapted from Shaw[2])

The pathway describes a 'perfect storm' where individuals with pre-existing personal vulnerabilities go on to experience stress events in their lives. These stressors can lead to concerning behaviours in the workplace, which if not dealt with effectively, may lead to an insider act.



The majority of people who appear on the pathway will not go on to become insider threats. Some people may become disengaged while at different stages on the pathway. They may start displaying other counter-productive workplace behaviours such as disgruntlement or they simply opt to leave the organisation.

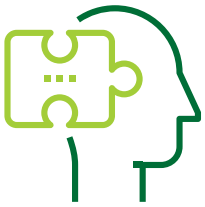
Organisations need to carefully consider their response as either overreacting or underreacting could either exacerbate or accelerate an individual along the pathway to insider risk. Positive interventions, however, can have the effect of diverting someone people off the pathway before an insider threat emerges or escalates. Such interventions could include a timely support from a line manager or a referral to wellbeing services.

Organisations should review how effective their current response is and plan improvements to reduce risk of escalation along the critical pathway.

Provide robust support mechanisms, such as mental health and wellbeing programmes, can help employees manage personal stressors. Normalising these services by removing any stigma is another way to promote early disengagement.

2 *See Shaw and Sellars reference p.9.*

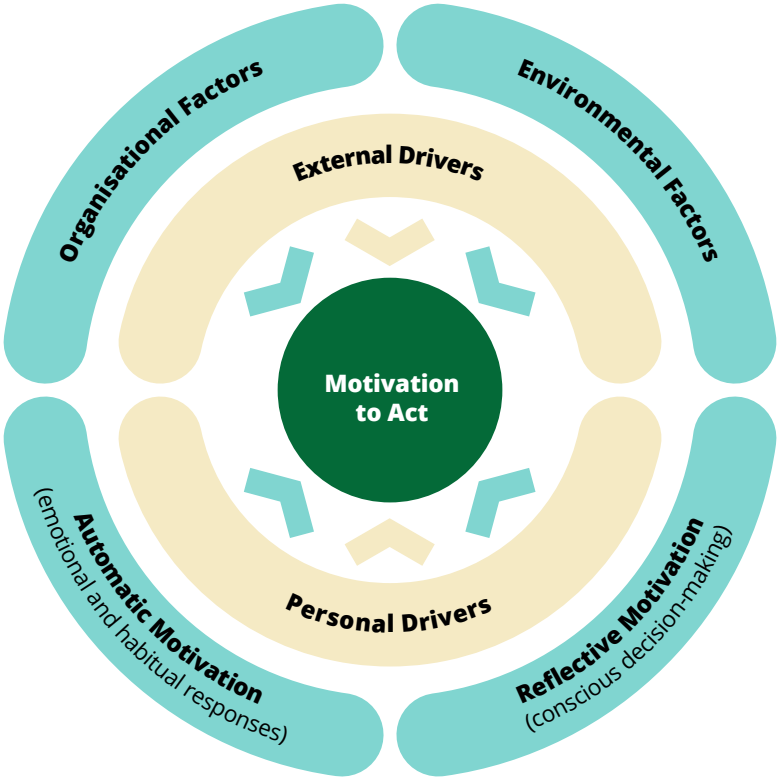
Principle 5
Learn the foundations for effective interventions



If you have people, then you have an insider risk. Accepting that key premise is the perfect starting point for developing effective interventions.

Consider what drives insider risk and the various potential mitigations. Human motivations are complex and individuals responsible for insider acts may struggle to explain their behaviour.

Motivations are influenced by both personal and external drivers as highlighted in the diagram below. Personal drivers may be automatic and unconscious or reflective and conscious based on certain values or goals. External drivers may include organisational factors like views on senior management and wider environmental factors such as their personal finances or even their concerns about a global conflict.



Motivation alone is not enough to trigger behaviours associated with an insider act. The person needs to have the capability and skills to cause harm as well as the opportunity such as the access to crucial information or weak security practices.

Workplaces can be shaped in a way that limits the opportunities for intentional or unintentional insider act.

A strong security culture is key led by engaged managers who are well versed on concerning behaviours and activities and are trained to make positive interventions to disrupt potential insider risks.

Managing risk throughout the employment lifecycle

It is easier to make effective interventions if your organisation has personnel security measures in place throughout the staff lifecycle. Well-designed systems start at the pre-employment stage and continue throughout someone's employment.

This requires a cycle of assessing personnel security risks, managing those risks, and evaluating the effectiveness of the measures you have in place.

Assess: Assess the risks your organisation faces relating to employees, contractors and temporary staff so you can identify and implement security measures to lower that risk to an acceptable level.

Manage: Apply your security measures from the pre-employment stage until the moment they leave, and sometimes beyond. Develop a security culture where the behaviours you require are adopted by everyone.

Evaluate: Carry out regular reviews to determine whether you have the right systems and processes in place. De-brief after any 'near misses' and capture any lessons learned.

Inform: Use your findings to drive positive improvements and to inform how you conduct your next round of risk assessments.

Check your security culture

Key factors in organisations with strong security cultures:

- **Buy-in from the top** – the chief executive and senior leaders must be committed to effective security practices with strong governance from the Board.
- **Strong security awareness** – staff understand the risks faced by the organisation and they role they play in minimising them.
- **Security communications are clear** – policies and procedures are clearly outlined and the reasons are understood.
- **Staff wellbeing supported** – staff have support networks available to them and feel comfortable to report issues.
- **Concerning behaviour is managed** – tools are available to identify and support those demonstrating concerning behaviours and activities.
- **No blame culture** – reporting emerging concerns or near misses should be treated as a way of helping colleagues who might be at risk, rather than getting them into trouble.

Think about promoting a "security first" culture within your organisation. A security-first culture is one in which security is embedded in everyday behaviours, decision-making, and organisational processes. Employees at all levels understand their responsibility for protecting information and actively contribute to reducing security risks. Organisations that fail to do the basics well as those where security is treated as an afterthought or solely the responsibility of the IT team.

Further reading

The Protective Security website includes more information on how to manage personnel risk in your organisation.

Check out the advice for:

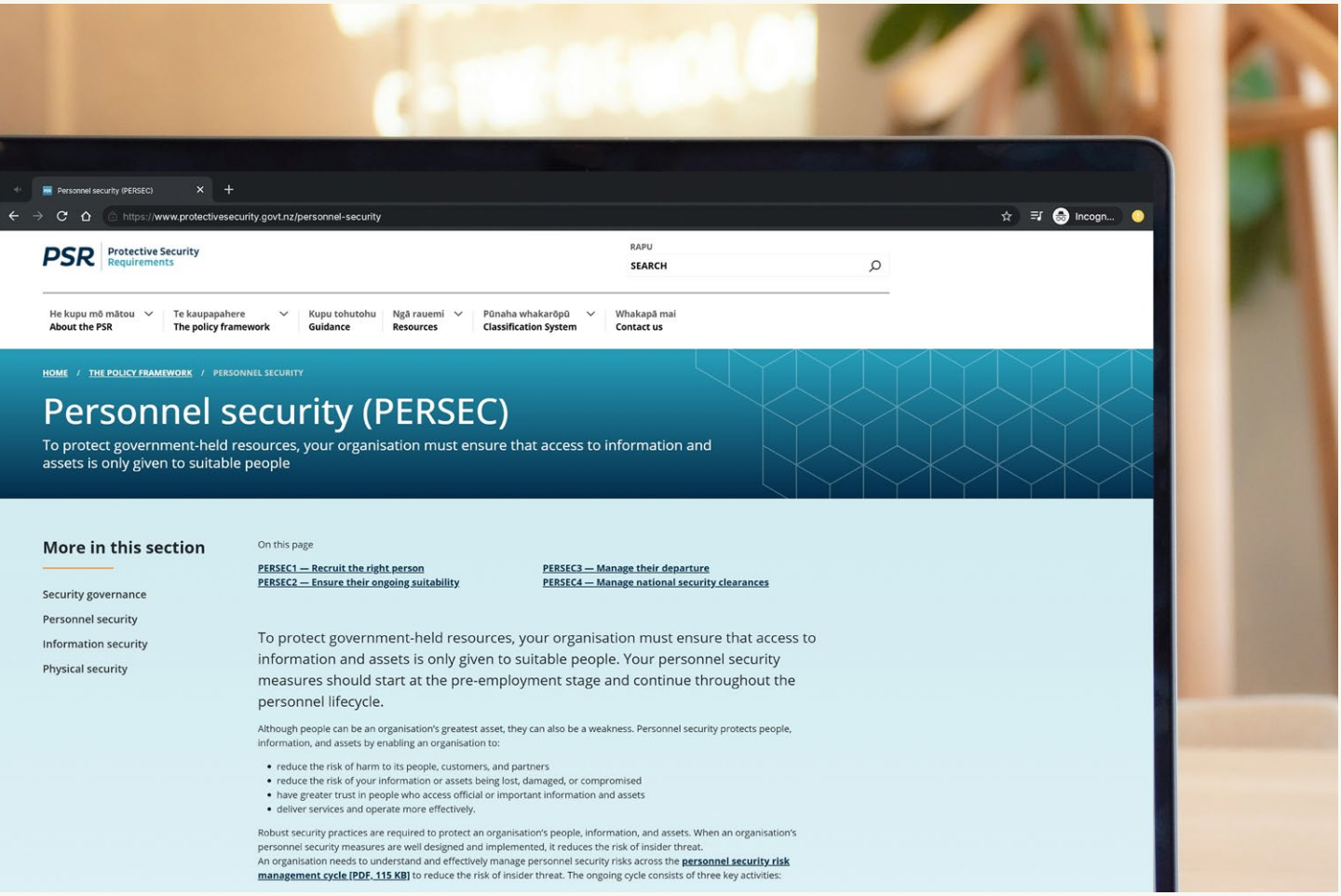
- Recruiting the right person
- Ensuring their ongoing suitability
- Managing their departure

Make sure access to information and assets is only given to suitable people.

Read more at: www.protectivesecurity.govt.nz/personnel-security

Understand the threat

Read the Insider Threat section in the latest New Zealand Security Threat Environment report at nzsis.govt.nz/threat-environment.



Te Pā Whakamarumaru
New Zealand Security
Intelligence Service