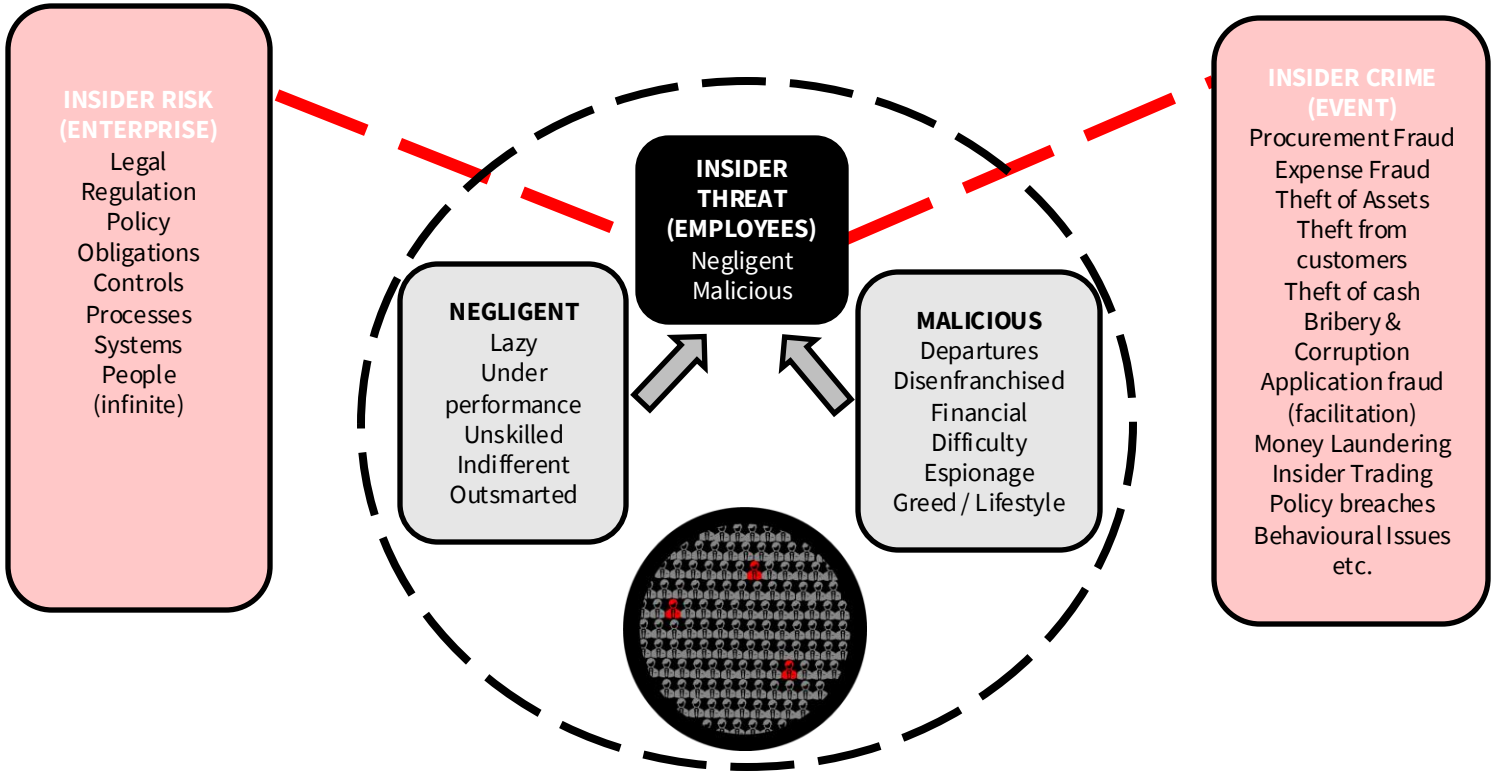
Trusted Insider Program

As criminals pivot to exploiting the most vulnerable, the instances of insider risk increases

Terminology - Risk – Crime -Threat



Trusted Insider Program – Purpose & Goals

Insider risk programs can identify and support at-risk employees, so they do not become threats (to the organisation or themselves)

The **Trusted Insider Program** aims to proactively detect, prevent, and manage employee-related risks that may threaten NAB's integrity or security. By addressing potential risks, we enable the broader workforce to operate confidently and securely.

By aligning teams across NAB who manage insider risks, the Trusted Insider Program will build a common understanding of threats, controls, and roles, enhancing our collective ability to address and uplift insider risk practices.

Insider Risk Framework – starts with the Board

Insider Risk Governance

Framework / Guidelines (policy) / Reporting / Executive accountability

Chairperson: Insider Risk Forum

Business Divisions	Financial Crime Risk Mitigation	Group Security	Compliance	People & Culture	Enablement
Personal Business Corporate Digital	Group Investigations	Data Protection Cyber Defence	Control Room Market Surveillance	Employee Relations Conduct Management	Offshore Businesses

Detection

Specific scenarios / behavioural monitoring

Incident Response

Event management / Investigation / Reg reporting / LEA contact

Control environment

Risk Mitigation / Prioritisation of uplift

Employee Lifecycle Stages – Insider Risks

Recruitment

Targeted candidates, 'Princeling' hires, falsified credentials, false identities, resume scanning

Pre-Employment

Background check gaps, conflicts of interest, identity

Onboarding

Access provisioning, compliance & security training

Ongoing

External targeting/collusion, employee stressors, disgruntlement

Offboarding

Delayed Access revocation, entitlement behaviour, data exfiltration, sabotage

Post Employment

Use of proprietary knowledge

Insider Threat – Individual Level

Who	Stressors	Pathway	Outcome
Opportunistic Insider Long term, trusted employee	Employee experiences financial difficulties, marriage breakdown, suffering grief, develops gambling/drug addiction, depression	Employee is opportunistic and exploits their access and system knowledge	Theft, fraud, bribery – whatever situation they can take advantage of and presents to them Typical examples include lending fraud, iCARE fraud, interest/fee refunds, falsifying records for sales commissions, false overtime Can include intellectual property theft, scouring GRACE for records of system vulnerabilities, data theft. Could become a vector for cyber intrusion or system manipulation
Disengaged Insider High performer	Employee perceives unfair treatment, passed over for a promotion, loses trust and becomes disengaged	Employee is resentful, disengages from NAB values and exploits legitimate access for personal or retaliatory purposes	
Compromised Insider Employee under pressure or exploited due to vulnerability	Threat actors target the employee through sextortion and psychological manipulation. They may exploit overseas family ties to coerce employees into cooperation	Employee is compromised and leveraged by an external party, using legitimate access under pressure or coercion	
Recruited Insider Employee knowingly collaborates with an external actor	False identification of employee that is really acting under instruction from state based actor or organised crime group	Employee is deliberately recruited and willingly exploits legitimate access to support external objectives	

Insider Risk – Sources of Increased Risk

"By understanding the drivers behind risky behaviour, we can identify key indicators to detect, deter, and support employees effectively."

Motivator	Example Key Risk Indicators
Personal Stressors Financial hardship due to personal circumstances or life events, such as divorce, gambling, addiction disorder, medical expenses, domestic violence, cost of living increases, or other events.	*Changes in behaviour, absenteeism, decline in performance, financial stress indicators, erratic work times*
Existing Employee Recruited by Adversary Legitimate employee targeted for recruitment by an external actor, such as a criminal enterprise or state-based actor, exploiting vulnerabilities like financial distress, family overseas, or compromising information.	*Family/close ties to overseas, travel to high-risk countries, unexplained wealth, interest in areas outside their role, changes in attitudes*
Employee Planted by Adversary Individual who has sought employment at NAB specifically to gain access to systems and data on behalf of a criminal enterprise or state-based actor.	*Remote work patterns, behavioural changes between recruitment & onboarding, unusual cyber activity, unexplained wealth, interest in areas outside their role*
Disgruntlement or Workplace Conflict Employee dissatisfaction due to perceived or actual treatment by NAB, such as organizational changes, conduct management, or performance management, that may lead to a feeling of entitlement	*Precipitating workplace event, change in behaviour, absenteeism, decline in performance, change in attitude, searching for new jobs*
Perceived Right to Retain Proprietary Information/Intellectual Property Employee who is leaving the organization and feels entitled to take property, information, or data to assist in a new role or organization.	*Searching for new jobs or tendered resignation, increase in activity during notice period, sending information outside organisation*
Ideologically motivations Employee holds ideological or political views that motivate them to act against NAB.	*Change in behaviour and attitudes, expressing unusual/fringe views, interest in areas outside their role*

Case studies