



Australian Institute
of Insider Threats

INSIDER THREAT CAPABILITY ASSESSMENT

Understand your Organisation's True Capability to Prevent,
Detect, Deter, and Respond to Insider Threats

HOW EXPOSED IS YOUR ORGANIZATION TO INSIDER THREAT-REALLY?

Most organisations invest heavily in controls, policies, and security tools.

Far fewer understand their **true capability** to manage insider threats when they occur.

Insider threats rarely begin with obvious wrongdoing. They emerge through trusted people, legitimate access, and small warning signs that are missed, normalised, or misunderstood.

They fail in the gaps between:

- Who owns insider threat decisions
- How early concerns are recognised
- How access is granted and removed
- How quickly issues are escalated and ‘
- How confidently the organisation can respond

By the time an insider incident becomes visible, the damage is often already done.

Most organisations don't lack tools. What they really lack is coordination, clarity, confidence and readiness across the full insider threat lifecycle.

THE INSIDER THREAT CAPABILITY ASSESSMENT

The Insider Threat Capability Assessment provides an independent, organisation-wide view of your organisation's ability to **prevent, detect, deter, and respond to insider threats.**

It examines how effectively your organisation brings together:

- Governance and leadership oversight
- Workforce awareness and culture
- Detection and monitoring practices
- Access management and privilege control
- Incident response and escalation
- Program maturity and continuous improvement
- Trust, fairness, and psychological safety

Together, these elements determine whether insider threats are managed as a true organisational capability or left to fail quietly between functions.

WHAT YOU RECEIVE

At the conclusion of the assessment, you receive a focused executive package designed to support confident decision-making:

Insider Threat Capability Maturity Rating

A clear view of how prepared your organisation truly is across prevention, detection, deterrence, and response, not just how many controls exist.

Identified Gaps and Blind Spots

Specific areas where current practices, ownership, or coordination increase the likelihood that an insider threat could go undetected or poorly managed.

Breakdowns in Ownership and Escalation

Where decision rights, accountability, or escalation pathways are unclear, delayed, or inconsistent in practice.

Prioritised Uplift Roadmap

A practical, phased set of recommendations showing:

- What matters most to fix first
- What can wait and

Where small changes will deliver the greatest reduction in insider threat exposure.

Executive Summary and Board-Ready Findings

A concise summary suitable for boards and senior leadership, translating technical and behavioural issues into clear governance and risk insights.

Executive Debrief Session

A confidential session to walk through the findings, discuss implications for leadership, and agree on realistic next steps.

HOW THE ASSESSMENT WORKS

The Insider Threat Capability Assessment is delivered through a structured, low-disruption process designed to provide executive assurance without placing unnecessary burden on the organisation.

Discovery, Alignment & Workshop

We begin with a structured engagement with key stakeholders to confirm objectives, organisational context, key risks, strengths, and improvement opportunities. This ensures the assessment is scoped and aligned to leadership expectations.

Structured Capability Assessment

Relevant leaders and subject-matter experts complete a guided assessment across seven capability domains. This captures how insider threat prevention, detection, deterrence, and response operate in practice across the organisation.

Executive Report & Debrief

Findings are consolidated into an executive report, followed by a confidential debrief session to discuss results, implications for leadership, and realistic next steps.

Typical timeframe: 4–6 weeks

Note: No personal data is collected. The process is designed to ensure confidentiality, fairness, and minimal disruption to operations.

WHO THIS ASSESSMENT IS FOR

This assessment is designed for organisations where an insider threat would have **material consequences** for operations, reputation, safety, or public trust.

It is particularly suited to:

- Boards and executive leadership teams seeking independent assurance
- Chief risk, security, governance, and compliance leaders
- Large, complex, and regulated organisations
- Environments with high trust, high access, and sensitive information
- Organisations strengthening governance, resilience, or assurance

It is most valuable for leaders who want:

- A clear view of how prepared the organisation truly is
- Confidence in their current posture and
- A defensible basis for prioritising capability uplift over time.



Australian Institute
of Insider Threats

NEXT STEP

If you would like to understand whether this assessment is suitable for your organisation, we recommend a short, confidential discussion.

In this initial conversation, we will:

- Understand your organisational context and priorities
- Discuss the types of insider threat challenges most relevant to you
- Explain how the assessment would be applied in your environment
- Outline scope, timeframe, and approach, and
- Confirm whether this is the right starting point for you.

This is a no-obligation discussion, designed to help you decide whether the assessment would provide value for your organisation.

Book a confidential consultation



<https://calendly.com/insider-threats/it-assessment-discussion>

Reach out to our staff: +61 2 6198 3381

WW.INSIDERTHREATS.COM.AU