GenerationAI

Shadow AI Risk Diagnostic Summary Report

Prepared for: Accretive AI

Assessment Completed By: Caleb John Lucas

Understanding What's Already Happening

AI is already active in your organisation, whether you've approved it or not. Staff are experimenting with tools like ChatGPT, Claude, and others to solve real problems faster. This hidden, unsanctioned use is known as Shadow AI.

This isn't rebellion, it's initiative. But when AI is used without leadership visibility, four serious risks emerge: sensitive data exposure, quality and accuracy issues, cybersecurity vulnerabilities, and a breakdown of trust between teams and leadership.

This diagnostic surfaces your hidden risks and shows clear steps to move from exposure to control.

As a **Healthcare** organisation with **1–10** employees, your Shadow AI risk profile has been assessed based on your current practices and organisational readiness.

Your Shadow AI Assessment

AREA	YOUR STATUS	RISK LEVEL
AI Tool Access	No access yet	Medium
Approval Process	Partial control	Medium
Detection Capability	Trust-based	High
Policy & Guidance	Verbal-only	Medium
Staff Training	Passive awareness	Medium
Data Exposure Risk	Uncertain	Medium
Accountability (Trace)	Some traceability	Medium
Compliance Awareness	Basic awareness	Medium
Previous Incidents	Suspected issues	Medium

What Each Area Means for Your Organisation

AI Tool Access

Without approved AI tools, staff find their own solutions. The gap between AI demand and approved supply is where Shadow AI thrives - every team without proper tools is likely using personal ChatGPT, putting data and IP at risk invisibly.

What you told us: You're actively considering AI tool access, but nothing is available yet. This delay increases the risk that staff begin using personal AI tools — often invisibly — to stay productive in the meantime.

Approval Process

Clear approval processes prevent fragmented tool selection. Without defined pathways, staff ask forgiveness not permission - Shadow AI fills the gap when governance is slow or unclear, creating uneven risk across teams.

What you told us: Some AI tools have been approved, but there's no formal process in place. That means approvals are likely happening ad hoc, which makes risk harder to monitor, manage, or explain.

Usage Visibility & Detection

Shadow AI spreads invisibly. Without knowing what tools are being used or having detection capability, you're flying blind - unable to manage risk, ensure compliance, or guide safe usage until an incident forces discovery.

What you told us about visibility: Shadow AI is now the norm, most staff are using personal tools that aren't approved or monitored. That's high exposure: you can't manage what you don't control.

What you told us about detection: Right now, you rely on staff honesty rather than systems to flag AI use. That's a major visibility gap, and it increases the risk of unintentional exposure, especially when tools are used without approval or oversight.

Policy & Training Foundation

Policy sets boundaries, training builds capability. Without both working together, staff either guess the rules or stay silent. Clear policy with proper training prevents Shadow AI from filling the gaps.

Your policy status: You rely on informal guidance rather than a documented policy. That helps in the short term, but informal rules are often applied inconsistently, especially as teams grow or change. Staff need clarity on what's okay and what's not.

Your training approach: The policy has been shared, but no training has been delivered. That creates a gap, people may agree in theory but still act unsafely in practice. Training turns policy into behaviour.

Data Exposure & Accountability

Once data enters public AI tools, you can't get it back. Without traceability, you can't answer the critical questions: Did AI touch this data? Can we prove what happened when clients or regulators ask?

Data exposure status: You're not sure whether data has been entered into public AI tools, that uncertainty is a risk in itself. It often means policies aren't reinforced through training or visible systems, making exposure harder to detect.

Traceability capability: You have some visibility into which AI tools are being used with customer data, but not full traceability. That makes it hard to give reliable answers if customers or regulators ask for specifics.

Compliance Awareness

AI tools processing customer or staff data trigger NZ Privacy Act obligations, even for small experiments. Ignorance isn't a defence. Unintentional breaches still bring penalties, regulatory scrutiny, and reputational damage.

What you told us: You've got some awareness of your legal obligations, but not full clarity. This uncertainty leaves you exposed, especially if staff are using AI tools in ways you can't monitor or trace.

Your Shadow AI Risk Profile

Previous Incidents: You suspect there may have been an AI-related issue, but nothing was confirmed. That uncertainty signals low visibility — which is itself a risk. If something did go wrong, it might still be unknown today.

Your Shadow AI Risk Score: 91/100

Your Next Steps: From Shadow to Strategy

Regardless of your current maturity level, strong AI governance rests on four foundations:

Core Foundations:

- **Clear ownership** - Someone must be accountable for AI strategy and risk
- **Visible guidelines** - Staff need to know what's approved and what's not
- **Regular review** - AI tools and risks evolve monthly, governance must keep pace
- **Staff capability** - Training and support turn policy into practice

Where you stand today: Unmanaged

What this means: Your organisation demonstrates strong AI governance practices with formal policies, training, and technical controls in place. Focus on continuous improvement and staying ahead of emerging risks.

Ready to Take Action?

Whether you're starting from scratch or optimising what's working, we can help.

AI Readiness Assessment & 90-Day Roadmap

Move from insights to action with a practical plan tailored to your organisation's specific situation and maturity level.

Book Your Session | **Learn More**

Supporting Resources

Access our guides and tools to support your AI readiness journey.

Explore Resources

Culture moves first. AI adoption only succeeds when your people are ready before your tools. GenerationAI specialises in helping organisations build the foundation for safe, strategic AI adoption that drives real business value.

Important Disclaimers

This assessment is based on information provided during completion and represents a point-in-time snapshot of your organisation's Shadow AI risk profile. Results depend on the accuracy and completeness of responses provided.

GenerationAI cannot assess risks or activities not disclosed during the diagnostic process. This diagnostic is designed to build awareness and guide strategic thinking about AI readiness and risk management.

This report does not constitute legal, compliance, or technical advice. Organisations should seek appropriate professional guidance for specific legal, regulatory, or technical requirements.

GenerationAI helps NZ organisations build AI capability through proven frameworks, practical tools, and strategic guidance. We specialise in moving businesses from AI exposure to AI advantage.