BUSINESS AI ASSESSMENT

KINETICS GROUP
making IT work for you

Your staff are already experimenting with AI. The opportunity is to make it safe and successful, and a driver of better business results.

AI is already in use. Now make it safe, visible, and useful.

We identify where AI is being used, what risks need guardrails, and the roadmap to move from experimentation to confident adoption.

WHAT WE ASSESS

01
Business Assessment

Goals, risks, current AI activity, approved tools, and governance maturity.

02
Data Assessment

Microsoft 365 security, sharing, sensitivity, DLP, and Copilot readiness.

03
User Assessment

Staff survey, endpoint scan, Asses training needs. Shadow IT survey to identify actual AI use in your business.

WHAT THE REPORT MAKES VISIBLE

AI Risks Found
Shadow AI, data sharing, policy gaps, training needs, and security posture.

Roadmap Delivered
Prioritised must-do and should-do actions with ownership and next steps.

Executive-ready Report
Clear findings, visuals, appendices, and board-friendly recommendations.

WHAT YOU RECEIVE

Current State	Findings	Roadmap
AI usage, tools, readiness, and key risks	Survey results, Shadow AI, Copilot, and security insights	Must-do and should-do actions with next steps

A PREVIEW OF YOUR REPORT



1. Executive Summary

This report presents the findings of the Business AI Assessment for [Client Name]. The assessment examined AI readiness across three dimensions (the business, the Microsoft 365 data estate, and the user base) to determine how safely and effectively AI tools such as Microsoft 365 Copilot can be adopted.

Overall AI readiness: DEVELOPING. NOT YET READY FOR BROAD ROLLOUT

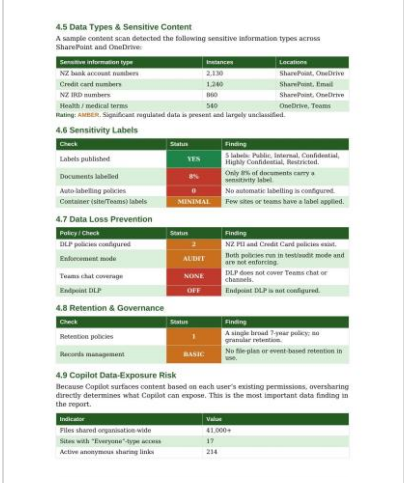
The licensing foundation for Copilot is largely in place. There are, though, significant data-governance gaps: widespread external and organisation-wide sharing, very low sensitivity-label coverage, and Data Loss Prevention policies running in audit-only mode. Together these mean that enabling Copilot broadly today would risk surfacing sensitive and over-shared content to users who should not see it. We recommend a focused remediation phase before broad rollout, with the option of a tightly-governed pilot for a small group in parallel.

Readiness scorecard

Readiness Domain	Rating	Summary
Business alignment & sponsorship	AMBER	Clear executive interest; AI strategy and governance not yet formalised.
Licensing readiness	GREEN	108 of 124 users hold Copilot-eligible licences.
Identity & security	AMBER	MFA at 78%; legacy auth still permitted; admin count above recommended.
Data security & external sharing	RED	Anonymous "Anyone" links enabled; 17 broadly-shared sites.
Information governance (labels / DLP / retention)	RED	Labels at 8% coverage; DLP in audit mode; minimal retention.
Copilot data-exposure risk	RED	High oversharing. Copilot would surface over permissioned content.
User adoption & skills	AMBER	Strong appetite; unmanaged "shadow AI" already in use.

Headline recommendations

- Do not enable Copilot tenant-wide until data oversharing and labelling are remediated.
- Remove anonymous "Anyone" sharing links and review the 17 broadly-shared sites.
- Move existing DLP policies from audit to enforce, and extend coverage to Teams and endpoints.
- Roll out and auto-apply sensitivity labels to lift coverage from 8% toward a target of 80%+.
- Establish an AI acceptable-use policy to bring "shadow AI" usage under governance.
- Begin a controlled Copilot pilot with a small, well-governed user group while remediation proceeds.



4.5 Data Types & Sensitive Content

A sample content scan detected the following sensitive information types across SharePoint and OneDrive:

Sensitive information type	Instances	Locations
NZ bank account numbers	2,130	SharePoint, OneDrive
Credit card numbers	1,240	SharePoint, Email
NZ IRD numbers	860	SharePoint, OneDrive
Health / medical terms	540	OneDrive, Teams

Rating: AMBER. Significant regulated data is present and largely unclassified.

4.6 Sensitivity Labels

Check	Status	Finding
Labels published	YES	5 labels: Public, Internal, Confidential, Highly Confidential, Restricted.
Documents labelled	8%	Only 8% of documents carry a sensitivity label.
Auto-labelling policies	0	No automatic labelling is configured.
Container (site/Teams) labels	MINIMAL	Few sites or teams have a label applied.

4.7 Data Loss Prevention

Policy / Check	Status	Finding
DLP policies configured	2	NZ PII and Credit Card policies exist.
Enforcement mode	AUDIT	Both policies run in test/audit mode and are not enforcing.
Teams chat coverage	NONE	DLP does not cover Teams chat or channels.
Endpoint DLP	OFF	Endpoint DLP is not configured.

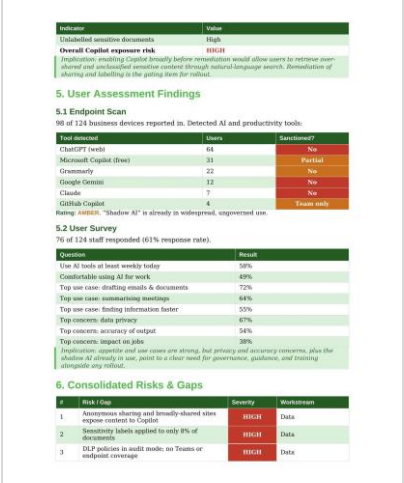
4.8 Retention & Governance

Check	Status	Finding
Retention policies	3	A single broad 7-year policy; no granular retention.
Records management	BASIC	No file-plan or event-based retention in use.

4.9 Copilot Data-Exposure Risk

Because Copilot surfaces content based on each user's existing permissions, oversharing directly determines what Copilot can expose. This is the most important data finding in the report.

Indicator	Value
Files shared organisation-wide	41,000+
Sites with "Everyone"-type access	17
Active anonymous sharing links	214



Indicator	Value
Unlabelled sensitive documents	High
Overall Copilot exposure risk	HIGH

Implication: enabling Copilot broadly before remediation would allow users to retrieve over-shared and unclassified sensitive content through natural-language search. Remediation of sharing and labelling is the gating item for rollout.

5. User Assessment Findings

5.1 Endpoint Scan

90 of 124 business devices reported in. Detected AI and productivity tools:

Tool detected	Users	Sanctioned?
ChatGPT (web)	64	No
Microsoft Copilot (free)	31	Partial
Grammarly	22	No
Google Gemini	12	No
Claude	7	No
GitHub Copilot	4	Team only

Rating: AMBER. "Shadow AI" is already in widespread, ungoverned use.

5.2 User Survey

76 of 124 staff responded (61% response rate).

Question	Result
Use AI tools at least weekly today	58%
Comfortable using AI for work	49%
Top use case: drafting emails & documents	72%
Top use case: summarising meetings	64%
Top use case: finding information faster	55%
Top concern: data privacy	67%
Top concern: accuracy of output	54%
Top concern: impact on jobs	38%

Implication: appetite and use cases are strong, but privacy and accuracy concerns, plus the shadow AI already in use, point to a clear need for governance, guidance, and training alongside any rollout.

6. Consolidated Risks & Gaps

#	Risk / Gap	Severity	Workstream
1	Anonymous sharing and broadly-shared sites expose content to Copilot	HIGH	Data
2	Sensitivity labels applied to only 8% of documents	HIGH	Data
3	DLP policies in audit mode; no Teams or endpoint coverage	HIGH	Data

Report includes: executive summary • current-state scorecard • staff survey insights • Shadow AI usage • Copilot readiness • adoption roadmap

INVESTMENT

Engagement setup & business assessment	**$2,500**
Discovery tools: endpoint scan & user survey	**$35 per user**
Analysis, reporting & presentation	**$2,200**
Total (excl. GST)	**$4,700 + $35/user**

All fees exclude GST. The per-user component is confirmed once the in-scope user population is agreed.

www.kinetics.co.nz or phone 0800 kinetics