AI Risk Scorecard

Sanitised sample extract | One page of a full audit deliverable

Client	Sector	Headcount	Audit date
Composite (identity redacted)	Manufacturing / industrial trades	~60 staff (AU, single site)	Redacted

Scope. Review of AI tool usage, governance practices, and decision risk. Informed by the AICD and HTI *Director's Guide to AI Governance* (eight elements of safe and responsible AI governance) and the *AI Governance Checklist for SME and NFP Directors*, applied within the Australian Privacy Principles (APPs) context. **This is not legal advice.** Findings flag exposure against named obligations so the organisation can engage appropriate counsel.

Governance	Data	Operations	Policy
RED	RED	AMBER	RED

#	Finding	Obligation flagged	Rating	Routing
01	**Customer enquiry data routed through Zapier to an external LLM** Marketing has built an automation that forwards inbound enquiry content (including names, phone numbers, project descriptions) to a third-party AI summariser. No privacy assessment on record. No customer notice. Data flow crosses jurisdictions.	APP 8 (cross-border disclosure); APP 1 (open and transparent management); APP 5 (notification of collection). AICD/HTI Eight Elements: Supporting infrastructure (AI inventory, data governance).	RED	Engage privacy counsel to review APP 8 obligations. Data flow and customer notification to be assessed before further use is decided.
02	**Unmanaged use of free-tier generative AI by admin and sales staff** Seven staff confirmed routine use of free public AI tools for drafting quotes, customer emails, and internal notes. No account governance. No record of what has been entered. No enterprise tier.	APP 11 (security of personal information). AICD/HTI Eight Elements: Practices, processes and controls; People, skills and culture.	RED	Exposure sits with executive leadership. Enterprise-tier options and interim usage position require assessment before further use is relied on.
03	**AI-generated marketing content published without human review gate** Website copy, product descriptions, and social posts are being generated by AI and published directly by the marketing coordinator. No review step. No fact-check. Two product spec inaccuracies identified during discovery.	ACCC guidance on misleading representations; directors' duty of care and diligence. AICD/HTI Eight Elements: Practices, processes and controls.	AMBER	Exposure sits with marketing and legal. Review gate design and publishing controls require assessment before further AI-assisted content is relied on.
04	**No responsible AI usage policy. No nominated accountable owner.** No written policy exists. No staff training. No nominated executive sponsor for AI decisions. Board minutes do not reflect AI as a standing item.	AICD/HTI Eight Elements: Roles and responsibilities; Principles, policies and strategy; Governance structures. SME/NFP Checklist pillar: Foundations.	RED	AICD/HTI Eight Elements assessment recommended across Roles and responsibilities, Principles policies and strategy, and Governance structures. Template policy supplied as a starting point for leadership and counsel to review.

What the full audit deliverable includes

This sample shows **one page** of the risk scorecard. The full audit also includes: a prioritised strategic action plan, a responsible AI usage policy template customised to your organisation, and a documented risk register mapped to the AICD/HTI eight elements of AI governance and relevant Australian Privacy Principles. Delivered within the agreed timeframe following the 90-minute discovery call.