

Thirteen AI Risks for Your Risk Register

Most risk registers we see have one line for AI, usually under cyber. That’s not enough to govern it. Here are thirteen entries you can copy into your register, rate against your own likelihood and consequence scale, and assign. Not every one will apply to you, and that’s a useful conversation in itself.

How to Use It

Table the list at your next audit and risk meeting. Ask management to bring back ratings, owners and controls by the following meeting.

Where to Start

Risks 1, 2 and 4 are the ones most organisations will rate highest right now. Risk 2 has a hard date: the automated decision-making obligation starts on 10 December 2026.

Don't Skip Risk 11

Missing the opportunity is the one most registers leave out. It keeps the conversation from becoming purely defensive.

No Committee?

Each risk carries a suggested owner. If you don't have that committee, the board owns it.

#	Risk	What could go wrong	Controls to consider	Suggested owner	Your assessment
1	Unapproved AI use Rate high now	Staff put personal, confidential or commercial information into personal AI accounts outside our control	Anonymous usage survey, approved alternative tool, acceptable use guide, browser and app monitoring	Audit and risk	L _____ C _____ Owner _____
2	Privacy and automated decisions Rate high now	We breach the Privacy Act, including the transparency obligation for automated decisions from 10 December 2026	Map decisions about people that software shapes, update the privacy policy, privacy impact assessments for new AI	Audit and risk	L _____ C _____ Owner _____
3	Relying on wrong AI output	Inaccurate AI output ends up in board papers, advice, funding applications, care notes or client deliverables	Human review rules by document type, disclosure of AI use, spot audits	Executive, with clinical governance where relevant	L _____ C _____ Owner _____
4	AI agents and connected apps Rate high now	An AI agent, including a staff member's personal agent, or a connected app with broad access is misused or compromised, exposing data or taking unauthorised actions	Register of connected apps, least-privilege access, approval before agents connect to core systems	Audit and risk	L _____ C _____ Owner _____

#	Risk	What could go wrong	Controls to consider	Suggested owner	Your assessment
5	AI-enabled fraud and impersonation	Deepfake voice, video or email impersonating executives or suppliers leads to a fraudulent payment or data release	Call-back verification for payment and bank detail changes, staff awareness, finance controls	Finance and audit	L _____ C _____ Owner _____
6	AI inside existing software	Vendors switch on AI features in systems we already use, processing our data in ways we haven't assessed	Review vendor AI terms at renewal, default settings check, data processing agreements	Executive	L _____ C _____ Owner _____
7	Contract and confidentiality breach	Using AI on client, funder or partner data breaches contract terms on confidentiality or data handling	Contract clause review, data classification, approved-tool rules by data type	Executive	L _____ C _____ Owner _____
8	Unfair or biased outcomes	AI-shaped decisions about eligibility, hiring, pricing or service disadvantage some groups, creating discrimination and reputational risk	Testing before go-live, human review of adverse decisions, complaints monitoring	Whole board	L _____ C _____ Owner _____
9	Workforce and culture	Hidden AI use, uneven skills, or poorly managed role changes erode trust and productivity	Clear permission to use approved tools, training, consultation on significant changes to roles	People and culture	L _____ C _____ Owner _____
10	Trust and reputation	An AI error in public communications or service delivery damages the trust of clients, donors, residents or customers	Review of public-facing AI content, incident response plan that covers AI	Whole board	L _____ C _____ Owner _____
11	Missing the opportunity Often missed	We fall behind peers or competitors, or keep stretched staff on manual work that AI could safely reduce	AI included in strategy, a funded pilot with measured outcomes, an annual board discussion of value	Whole board	L _____ C _____ Owner _____
12	Board oversight gap	The board lacks the knowledge, information or reporting rhythm to oversee AI	Director education, AI reporting in the board calendar, a named executive owner	Chair	L _____ C _____ Owner _____
13	Recording and capture	AI glasses, pendant recorders or meeting notetakers capture clients, residents, staff or visitors without consent, breaching surveillance or privacy law	Recording policy for staff, visitors and contractors, notice and signage, rules for client and care settings	People and culture	L _____ C _____ Owner _____

L = likelihood, C = consequence, rated on your own scale. "Rate high now" and "Often missed" labels reflect what we see across organisations, not your organisation's position.

If you'd like help running an anonymous AI usage survey or mapping your automated decisions before 10 December, get in touch and we'll set up a conversation. And if you think we've got something wrong, we'd like to hear that too.

