

AI risk assessment

One assessment per AI tool or use. Fill in the parts in square brackets, score each risk, and agree a measure for anything rated 6 or above before the tool goes live. Review it when anything changes. It isn't legal advice.

AI tool or use	[What it is, and the supplier]
Owner	[Name, role]
Assessed by	[Name, role]
Date	[DD/MM/YYYY]

1 The tool and the job

What it does	[The job, in a sentence]
Who uses it	[Team, roughly how many people]
What goes in	[Documents, emails, recordings, and any personal data]
What comes out	[Drafts, summaries, answers, and who sees them]
The supplier	[Who runs it, what they keep, where it's processed]
Who checks the output	[Name or role]

2 How to score

- Likelihood: 1 unlikely, 2 possible, 3 likely.
- Impact: 1 minor, 2 serious, 3 severe.
- Rating: likelihood times impact, from 1 to 9.
- 6 to 9 is high: agree a measure before go-live. 3 or 4 is medium: agree a measure and a date. 1 or 2 is low: note it and review.

3 Risk register

Risk	Likelihood 1 to 3	Impact 1 to 3	Rating 1 to 9	Measure	Owner
A wrong or made-up output is used without being checked					
Personal or confidential data goes in that shouldn't					
People can see documents through the tool that they couldn't open before					
The supplier keeps inputs, or uses them to train its models					
Data is processed or supported outside the UK without a safeguard					
Outputs treat some groups of people unfairly					
Instructions hidden in a document or email trick the tool into doing something it shouldn't					
The tool stops working or changes, and the job depends on it					
Running costs grow beyond the budget					
[Add your own]					

4 Sign-off

Approved by	[Name, role, DD/MM/YYYY]
Remaining high risks accepted by	[Name, role. If personal data is involved, check whether you need a DPIA]
Next review	[DD/MM/YYYY, or when the tool, supplier or use changes]