FREE RESOURCE · CAUTRA.IO

12-Point AI Risk Checklist

Audit your team's AI exposure in under 5 minutes.
12 yes/no questions. Every No is a gap to fix.

NIST AI RMF | CIS Controls v8.1 | EU AI Act 2026 | UK GDPR

12	5 MIN	4
YES/NO QUESTIONS	TO COMPLETE	FRAMEWORKS

HOW TO USE THIS CHECKLIST

Answer Yes or No to each of the 12 questions below.
Count your Yes answers. Find your score band on the final page.
Every No answer is a gap — the Cautra AI Risk & Policy Kit fixes all of them.

Questions begin on the next page →

CHECKLIST

The 12 Questions

Answer Yes or No to each question. A No answer means a gap — fix each one with the Cautra kit.

01 NIST AI RMF · MAP 1.1

AI TOOL INVENTORY

Do you have a written list of every AI tool your team uses — including free and personal accounts?

This includes ChatGPT, Copilot, Grammarly, Otter.ai, Midjourney, and AI features inside tools like HubSpot or Notion. If you can't list them all, you can't govern them.

Framework: NIST AI RMF: MAP 1.1 (Context established). CIS Controls v8.1: Control 1 (Asset Inventory). EU AI Act Art. 4 (AI literacy, Feb 2025).

YES ☐ NO ☐

02 NIST AI RMF · GOVERN 1.2

DATA CLASSIFICATION

Do you know what data classification applies to the information your team enters into AI tools?

Public, internal, confidential, or personal data carry different risk levels. Pasting a client NDA into free ChatGPT is a very different risk to drafting a generic email. If your team doesn't know the difference, they can't make safe decisions.

Framework: NIST AI RMF: GOVERN 1.2 (Policies established). CIS Controls v8.1: Control 3 (Data Protection). UK GDPR Art. 5 (data minimisation).

YES ☐ NO ☐

03 UK GDPR · Art. 28

PERSONAL DATA & GDPR

Is personal data (names, emails, employee records, client contact details) entering any AI tool?

If yes, you need a Data Processing Agreement (DPA) with that vendor before any personal data is processed. Without one, you are likely in breach of UK GDPR. Free AI tools almost never offer a DPA.

Framework: UK GDPR Art. 28 (processor contracts). EU AI Act deployer obligations. NIST AI RMF: GOVERN 6.1 (Third-party risk). CIS Controls v8.1: Control 15 (Service Provider Management).

YES ☐ NO ☐

04 CIS Controls · Control 14

ACCEPTABLE USE POLICY

Does your team have a written AI Acceptable Use Policy telling them what they can and cannot do?

Without a written policy, you have no documented basis for discipline if something goes wrong and no evidence of good-faith governance if a regulator asks. It doesn't need to be long — it needs to be clear.

Framework: CIS Controls v8.1: Control 14 (Security Awareness). NIST AI RMF: GOVERN 1.1 (Policies aligned to legal requirements). EU AI Act Art. 4 (AI literacy obligation, Feb 2025).

YES ☐ NO ☐

05 EU AI Act · Art. 4

STAFF AWARENESS

Has every team member received training on your AI policy and the risks of AI tool misuse?

EU AI Act Article 4 made AI literacy training a legal obligation for all organisations deploying AI in the EU as of February 2025. Training records must be maintained. This is not optional.

Framework: EU AI Act Art. 4 (AI literacy, in force 2 Feb 2025). CIS Controls v8.1: Control 14 (Security Awareness). NIST AI RMF: GOVERN 4.1 (Roles communicated).

YES ☐ NO ☐

06 CIS Controls · Control 15

VENDOR RISK

Have you reviewed the data handling and model training policies of the AI tools your team uses?

Free-tier AI tools often use your inputs to train their models. Enterprise plans typically opt out by default. You need to know which of your tools are which — and have the vendor's policy documented.

Framework: CIS Controls v8.1: Control 15 (Service Provider Management). NIST AI RMF: MAP 1.6 (Third-party risk assessed). UK GDPR Art. 28 (processor due diligence).

YES ☐ NO ☐

07

NIST AI RMF · MANAGE 2.2

AI OUTPUT REVIEW

Is there a process requiring human review of AI-generated outputs before they are used or shared?

AI tools can produce confident, plausible, and completely wrong outputs — known as hallucination. Any AI-generated document, analysis, or code used in a business context must be reviewed by a named person before use.

Framework: NIST AI RMF: MANAGE 2.2 (Human oversight mechanisms). MANAGE 4.1 (Post-deployment monitoring). EU AI Act deployer obligations Art. 26.

YES ☐ NO ☐

08

CIS Controls · Control 17

INCIDENT RESPONSE

Do you have a documented process for reporting and responding to AI-related security incidents?

An AI incident includes: pasting personal data into an unauthorised tool, an AI output causing harm, a vendor data breach, or an AI-enabled fraud attempt. Without a process, staff won't know what to report or who to tell.

Framework: CIS Controls v8.1: Control 17 (Incident Response). NIST AI RMF: RESPOND 1.1 (Incident response plans). UK GDPR Art. 33 (72-hour breach notification).

YES ☐ NO ☐

09

NIST AI RMF · MEASURE 2.5

AI RISK ASSESSMENT

Have you conducted a documented risk assessment covering AI-specific risks for your business?

A risk assessment identifies your highest-exposure scenarios — data leakage, shadow AI, hallucination in client work, AI-enabled fraud — and documents what controls you have in place. Without one, you have no baseline.

Framework: NIST AI RMF: MEASURE 2.5 (Risks documented). MAP 5.1 (Risk documentation). NIST CSF 2.0: GV.RM (Risk Management Strategy).

YES ☐ NO ☐

10

EU AI Act · Risk Tiers

EU AI ACT CLASSIFICATION

Have you assessed whether any AI tools you use fall into the EU AI Act's high-risk or prohibited categories?

Most productivity AI falls in the minimal-risk tier. AI used in hiring, credit decisions, or healthcare triage is high-risk with full compliance obligations. Prohibited AI practices must have been discontinued since February 2025.

Framework: EU AI Act Arts. 5–6, Annex III (risk classification). High-risk enforcement: Aug 2026. Prohibited practices: in force Feb 2025.

YES ☐ NO ☐

11

NIST AI RMF · GOVERN 6.2

IP & COPYRIGHT

Do you have a position on intellectual property ownership of AI-generated outputs used in your business?

AI-generated content may incorporate third-party material or face uncertain copyright status. If AI is used in client deliverables, your contracts should address this. Staff should not present AI outputs as original work without disclosure.

Framework: NIST AI RMF: GOVERN 6.2 (IP considerations). EU AI Act transparency obligations Art. 50. UK Copyright, Designs and Patents Act 1988 (AI-generated works).

YES ☐ NO ☐

12

NIST AI RMF · GOVERN 1.4

GOVERNANCE OWNERSHIP

Is there a named person in your organisation responsible for AI governance and policy compliance?

AI governance without an owner is not governance. Someone must own the AI asset register, review it quarterly, respond to tool approval requests, and keep the policy current. At a small team this is typically the founder, ops lead, or IT lead.

Framework: NIST AI RMF: GOVERN 1.4 (Roles and responsibilities assigned). CIS Controls v8.1: Control 1 (designated owner). EU AI Act deployer accountability obligations.

YES ☐ NO ☐

SCORE GUIDE

How to interpret your results

YES answers	Rating	What it means
0–3	HIGH RISK	Significantly exposed. Prioritise an AI Acceptable Use Policy and Tool Register immediately.
4–7	MEDIUM RISK	Good start — but gaps remain. Focus on the No answers first.
8–10	LOW RISK	Strong foundation. Review annually and whenever new AI tools are adopted.
11–12	WELL GOVERNED	Excellent. Consider the Cautra Pro Pack for deeper framework alignment.