AI readiness checklist (scored)

Company: _____ Completed by: _____ Date: _____

Answer each question Yes or No. A question scores 1 for Yes and 0 for No; each area is out of 5 and the total is out of 30. Answer Yes only if you can point to the evidence. There is no pass mark: every No is a gap to close. Close the No answers in Data and permissions, Identity and devices, and Regulatory scope before you give many people an AI assistant that can read company email, files or chats.

The six areas follow the CIO Support answer 'What is an AI readiness assessment and does my company need one?' (cio.support/ai/ai-readiness-assessment/). NIST's AI Risk Management Framework is voluntary and is not a checklist; this is a practical starting point, not a compliance standard, and it does not replace a review of your actual permissions, accounts and vendor terms.

#	Data and permissions	Yes	No	Evidence to look for	Evidence you have (where)
1	Have you reviewed which sites, shared drives and folders are open to everyone in the company or to large groups?	☐	☐	Permissions or sharing report (in Microsoft 365, the SharePoint data access governance reports)	
2	Have old company-wide and 'anyone with the link' sharing links been reviewed or removed?	☐	☐	Sharing-link report with the date it was reviewed	
3	Has guest and external-user access been reviewed, and stale guests removed?	☐	☐	Guest access review record	
4	Are the most sensitive areas (finance, HR, legal, research) limited to the people who need them?	☐	☐	Access list for each sensitive area	
5	Is confidential and regulated content labeled or otherwise identified?	☐	☐	Sensitivity label coverage report, or a list of where regulated data is kept	
	Data and permissions score (number of Yes answers)			**_____ / 5**	

#	Identity and devices	Yes	No	Evidence to look for	Evidence you have (where)
6	Does every account that will get AI access use multi-factor authentication?	☐	☐	MFA registration report	
7	Do approved AI tools sign in through your company identity, with single sign-on where available?	☐	☐	App list or SSO configuration in your identity provider	
8	Are departed users disabled promptly, and have accounts been reviewed in the last 90 days?	☐	☐	Offboarding checklist and the latest account review	
9	Are the devices people will use for AI work company-managed, or covered by a device policy?	☐	☐	Device management enrollment report	
10	Do you know which licenses each planned AI tool needs, and are the prerequisites in place?	☐	☐	Licensing and identity readiness checklist from the vendor	
	Identity and devices score (number of Yes answers)			**_____ / 5**	

#	Shadow AI	Yes	No	Evidence to look for	Evidence you have (where)
11	Do you have a list of the AI tools staff already use for work, including free and personal accounts?	☐	☐	Cloud discovery or AI usage report, or staff survey results	
12	Have you reviewed browser extensions and AI apps connected to company mail, files or calendars?	☐	☐	App consent (OAuth) report and extension inventory	
13	Have you checked expense and card records for AI subscriptions?	☐	☐	Expense review notes	
14	Do you know which AI features are switched on inside software you already use (CRM, help desk, meetings)?	☐	☐	List of enabled AI features per application	
15	Can you warn or block sensitive data going to unapproved AI sites on managed devices?	☐	☐	Data loss prevention policy or web filter rule	
	Shadow AI score (number of Yes answers)			**_____ / 5**	

#	Policy and governance	Yes	No	Evidence to look for	Evidence you have (where)
16	Is one named person accountable for decisions about AI use?	☐	☐	Name and role, in writing	
17	Is there a published AI acceptable-use policy that employees have acknowledged?	☐	☐	Signed policy and acknowledgment records	
18	Is there an approved-tools list with the highest data level allowed in each tool?	☐	☐	Approved-tools register	
19	Have each approved tool's vendor terms (training use, retention, data location) been reviewed?	☐	☐	Vendor review record with the date the terms were read	
20	Is there a route for reporting AI mistakes, and a set date to review the policy and tool list?	☐	☐	Policy reporting section and the review date on a calendar	
	Policy and governance score (number of Yes answers)			**_____ / 5**	

#	Regulatory scope	Yes	No	Evidence to look for	Evidence you have (where)
21	Do you know whether you hold protected health information, and is it kept out of AI tools that are not covered by a business associate agreement? (Answer Yes if you hold no protected health information.)	☐	☐	Business associate agreement, or a written decision that PHI stays out	
22	If your DoD contracts include DFARS 252.204-7012, have you confirmed which AI tools, if any, may process covered defense information? (Answer Yes if no contract or subcontract includes that clause.)	☐	☐	System security plan scope, or a written decision	
23	Is export-controlled (ITAR or EAR) technical data identified and kept out of unapproved AI tools?	☐	☐	Export-control review	
24	Have you checked customer and partner contracts for confidentiality terms or limits on AI use?	☐	☐	Contract review notes	
25	Life sciences: has your quality lead confirmed whether any AI use touches validated systems or GxP records? (Answer Yes if your company does no GMP, GLP or GCP work. If it does, answer Yes only when the quality lead has made the decision in writing.)	☐	☐	Quality decision record	
	Regulatory scope score (number of Yes answers)			**_____ / 5**	

#	Use cases and pilot	Yes	No	Evidence to look for	Evidence you have (where)
26	Have you listed candidate AI use cases with the business value of each?	☐	☐	Ranked use-case list	
27	For each use case, do you know what data it needs and how that data is classified?	☐	☐	Data column in the use-case list	
28	For each use case, have you set who reviews AI output and what an error would cost?	☐	☐	Human-review rule per use case	
29	Is there a pilot plan with a small group, low-risk data and a measure of success?	☐	☐	Pilot plan	
30	Is there a date to review pilot results and decide to expand, change or stop?	☐	☐	Calendar entry and decision record	
	Use cases and pilot score (number of Yes answers)			**_____ / 5**	

Summary

Area	Score
Data and permissions	_____ / 5
Identity and devices	_____ / 5
Shadow AI	_____ / 5
Policy and governance	_____ / 5
Regulatory scope	_____ / 5
Use cases and pilot	_____ / 5
Total	_____ **/ 30**

There is no pass mark. Every No is a gap to close; start with Data and permissions, Identity and devices, and Regulatory scope. The Excel version adds up the scores for you.