

DATA AND AI GOVERNANCE SELF-CHECK

About 20 minutes. Tick one box for each question about your own setup. Questions marked with a size apply from that size up; below it, answer only if they matter to you.

RoughDigits

1. Tick

Yes, Partly, No, or N/A (does not apply).

2. Count

2 points for each Yes, 1 for each Partly, 0 for each No.
Leave N/A out.

3. Score

Points divided by twice the number of questions you answered (not counting N/A).

#	Question	Yes	Partly	No	N/A	What to look at first, for a No or a Partly
1	KNOW YOUR DATA Do you have one list of every place your business data is kept: systems, shared drives, apps and laptops? Everyone	☐	☐	☐	☐	Start a one-page list: each place, what data it holds, and who owns it. Email, file storage and accounting are usually the first three lines.
2	KNOW YOUR DATA Do you know which personal data you hold (customers, staff, suppliers) and why you hold it? Everyone	☐	☐	☐	☐	Pick your three biggest systems and note which personal data each holds and why. Delete what you no longer need.
3	KNOW YOUR DATA Is your data sorted by how sensitive it is (for example public, internal, confidential), with a rule for each? 50+ people	☐	☐	☐	☐	Agree three or four labels and one rule per label, then apply them to the systems on your list, most sensitive first.
4	ACCESS: PEOPLE Does everyone sign in with their own account, with no shared logins? Everyone	☐	☐	☐	☐	Find shared logins (often social media, finance and admin tools) and give each person their own account.
5	ACCESS: PEOPLE Is multi-factor sign-in switched on for email and every system holding personal or client data? Everyone	☐	☐	☐	☐	Turn it on for email first, then for file storage, finance and any system on your list marked confidential.
6	ACCESS: PEOPLE When someone leaves or changes role, is their access removed within one working day? 10+ people	☐	☐	☐	☐	Write a short leaver checklist covering every system on your list, and give one person the job of running it.
7	ACCESS: PEOPLE Is access to important systems reviewed at least every six months? 10+ people	☐	☐	☐	☐	Ask each system owner to confirm who has access, and remove anyone who no longer needs it.

#	Question	Yes	Partly	No	N/A	What to look at first, for a No or a Partly
8	ACCESS: SYSTEMS Do you know which connected apps, integrations and service accounts can reach your data? Everyone	☐	☐	☐	☐	Open the admin settings of your email and file storage and look at the list of connected apps. Remove any nobody recognises.
9	ACCESS: SYSTEMS Are passwords and API keys for systems kept in a password manager or secrets vault, not in files, emails or chats? Everyone	☐	☐	☐	☐	Move shared passwords and keys into a password manager, then change the ones that were stored in plain text.
10	ACCESS: SYSTEMS Do automations and AI agents have their own accounts, with only the access they need? Everyone	☐	☐	☐	☐	List each automation or agent, the account it uses and what it can reach. Give each its own account and cut access it does not use.
11	AUDIT TRAIL Do your main systems record who and what read or changed data, and is that record switched on? Everyone	☐	☐	☐	☐	Check the audit or activity log settings in your email, file storage and main business system. Switch them on and keep them as long as the system allows.
12	AUDIT TRAIL Would you notice if a large amount of data were downloaded or shared outside the business? 10+ people	☐	☐	☐	☐	Turn on the sharing and download alerts your file storage and email already offer, and send them to a named person.
13	AUDIT TRAIL Does someone look at access and activity records at least once a month? 50+ people	☐	☐	☐	☐	Set a monthly half-hour to review sign-ins from new places, sharing outside the business and admin changes.
14	AI USE Do you have a list of the AI tools in use, including free ones people signed up for themselves? Everyone	☐	☐	☐	☐	Ask everyone, without blame, which AI tools they use and for what. Check card statements and sign-in records for more.
15	AI USE Is there a written rule on what must never go into AI tools? Everyone	☐	☐	☐	☐	Write one page: what never goes in (for example personal data, client confidential data, passwords and unreleased source code) and which tools are approved for what.
16	AI USE Is AI used through business accounts whose data terms you have read, rather than personal accounts? Everyone	☐	☐	☐	☐	For each AI tool on your list, check whether a business plan exists and what its terms say about keeping and using your data. Move work onto those accounts.
17	AI USE Do you know which AI features are switched on inside software you already pay for? Everyone	☐	☐	☐	☐	Check the AI settings in your email, office, customer and support software. Turn off what you have not approved.

#	Question	Yes	Partly	No	N/A	What to look at first, for a No or a Partly
18	AI USE Is there an approval step before a new AI tool is used or connected to company data? 10+ people	☐	☐	☐	☐	Name one person who approves new AI tools against your one-page rule, and tell everyone where to ask.
19	AI USE Have people been shown, in the last year, what is safe to put into AI? 10+ people	☐	☐	☐	☐	Run a 20-minute session using real examples from your own work, and share the one-page rule.
20	OWNERSHIP Is one named person responsible for data protection and AI use? Everyone	☐	☐	☐	☐	Name the owner. On your own, it is you: write it down anyway, with a date to review.
21	OWNERSHIP Do you have a plan for a data leak: who to tell, by when, and who does what? Everyone	☐	☐	☐	☐	Write a one-page plan: who decides, who you must tell (clients, regulators) and by when, and where the contact details are kept.
22	OWNERSHIP Do your security and governance people work from the same list of AI uses? 250+ people	☐	☐	☐	☐	Agree one shared register of AI uses, owned jointly, and review it together each quarter.

Your score

Points _____ divided by (2 x questions answered _____) = _____ %

Where you are

Under 40%: Early: start with your first three gaps
 40% to 74%: Developing: close the gaps needed at your size first
 75% and above: Established: keep it reviewed