

Shadow AI Visibility Checklist

Ten questions leadership should be able to answer. Check **YES** only when the answer is documented and current.

#	CONTROL	LEADERSHIP QUESTION	YES	NO
1	Inventory	Do we have a dated list of sanctioned, embedded, and employee-adopted AI tools?	☐	☐
2	Ownership	Does every AI tool have a named business owner accountable for its use?	☐	☐
3	Data	Do we know which tools receive client, employee, financial, regulated, or proprietary data?	☐	☐
4	Accounts	Can we distinguish managed business accounts from personal or consumer accounts?	☐	☐
5	Vendors	Have we reviewed privacy terms, DPAs, retention, training use, and sub-processors?	☐	☐
6	Policy	Do employees have a short, readable AI acceptable-use policy and sanctioned-tool list?	☐	☐
7	Review	Is human review required for client-facing, financial, legal, HR, or consequential outputs?	☐	☐
8	Intake	Is there a documented process for requesting and approving new AI tools or features?	☐	☐
9	Incidents	Can staff report an AI mistake or data exposure without guessing whom to contact?	☐	☐
10	Cadence	Is a quarterly AI inventory and risk review assigned and on the calendar?	☐	☐

8-10 YES	5-7 YES	0-4 YES
Visible foundation	Material gaps	Immediate blind spot
Validate the evidence and refresh quarterly.	Prioritize missing controls during the next 30 days.	Begin with an exposure scan before adding more AI tools.

This checklist is a visibility screen, not a compliance certification or legal opinion. Aegis AI Advisory can help verify the answers and turn the gaps into a prioritized action plan.