



AI Governance Readiness Checklist

Govern First. Architect Second. Automate Third.

A practical self-assessment for founders, leaders, and teams adopting AI. Allow 10-15 minutes for an initial pass; verify supporting evidence afterward.

Score every statement: **0 = absent or unsure; 1 = partial or informal; 2 = documented, in use, and supported by current evidence.**

If not yet using AI, score your preparations. Do not omit core items.

Organization / team: _____ Date: _____

01 | Ownership & accountability

Readiness statement	Score
01. A named leader owns AI governance and can approve, restrict, or stop AI use.	---
02. Each AI use case has a business owner and a documented purpose.	---
03. Written rules explain who approves tools, exceptions, and higher-risk uses.	---
04. Staff know how to report AI concerns and who must respond.	---

02 | AI inventory & risk

Readiness statement	Score
05. We maintain a list of AI tools, embedded AI features, users, and connected systems.	---
06. We assess potential harm to people, privacy, security, finances, and reputation before use.	---
07. We define approved, restricted, and prohibited uses, including higher-impact decisions.	---
08. We document expected benefits, success measures, and when AI should not be used.	---

03 | Data & access boundaries

Readiness statement	Score
09. Clear rules identify what data may enter each approved tool and what must stay out.	---
10. We verify rights and permissions to use personal, client, confidential, and copyrighted data.	---
11. Access is limited to what each person or tool needs and removed when no longer needed.	---
12. We document retention, deletion, storage, and provider training settings for our data.	---

Put governance into practice

Continue scoring: 0 = absent / unsure | 1 = partial | 2 = evidenced

04 | Tool & vendor review

Readiness statement	Score
13. Someone reviews vendor security, privacy, reliability, and contractual terms before approval.	---
14. We assess provider data sharing, subcontractors, and incident-notification commitments.	---
15. We understand tool limitations and test performance in our actual business context.	---
16. We can export needed records, revoke access, and switch providers or work manually.	---

05 | Human oversight & quality

Readiness statement	Score
17. A qualified person checks important outputs for accuracy, bias, and suitability before use.	---
18. Human approval is required before consequential decisions or sensitive external actions.	---
19. We test realistic failures and effects on affected groups, with documented acceptance criteria.	---
20. We define when to disclose AI use and how people can seek human review or correction.	---

06 | Training, monitoring & response

Readiness statement	Score
21. Staff receive role-specific training on AI rules, limitations, data handling, and escalation.	---
22. We keep appropriate records of approvals, tests, changes, and incidents with access controls.	---
23. We monitor results and reassess after model, tool, data, or workflow changes.	---
24. We have tested how to stop unsafe use, contain incidents, notify the right people, and recover.	---

Address these gaps first

Regardless of score, restrict the affected use until safeguards are in place if sensitive data enters unapproved tools, consequential actions lack human approval, or nobody can stop unsafe AI activity. Escalate suspected harm or exposure through your incident process.

Understand your result

Add the 24 core scores. Total: _____ / 48. Score each section out of 8 to see where help is most needed.

Score	Starting point	Next step
0-15	Build the foundation	Name an owner, inventory AI use, and establish data and approval rules.
16-31	Close operating gaps	Turn informal practices into documented controls and test them.
32-41	Strengthen consistency	Verify evidence, address weak areas, and improve monitoring.
42-48	Validate before expanding	Check controls against each intended use and review agent safeguards.

These are THBS planning bands, not validated maturity benchmarks. A high total cannot offset a serious control gap. This checklist is not a certification, audit, legal opinion, or authorization to deploy.

Additional check: AI agents

Complete this section if AI can call tools, send messages, modify records, or act across systems. Planning agents? Assess before deployment. No agents used or planned? Mark this section N/A. These items are not included in the 48-point total.

Agent safeguard	Ready?
A1 Limited authority Each agent has a named owner, defined purpose, allowed actions, and explicit prohibited actions.	Y/ P/ N
A2 Restricted access Separate credentials and least-privilege permissions limit which tools and records an agent can access.	Y/ P/ N
A3 Approval gates A person must approve payments, deletions, sensitive record changes, and consequential communications before execution.	Y/ P/ N
A4 Untrusted inputs Tests cover malicious instructions in emails, files, or web content that could redirect the agent or expose data.	Y/ P/ N
A5 Traceable actions Logs show tool calls, approvals, and outcomes without unnecessarily retaining sensitive information.	Y/ P/ N
A6 Stop & recover We have tested time, cost, and action limits, emergency shutdown, credential revocation, and recovery from partial failures.	Y/ P/ N

Y = evidenced and operating; P = partial; N = absent or unsure. Any P or N is a gap to resolve before granting the corresponding action or access.

Turn gaps into next steps

Choose three priorities. Start with potential harm, data exposure, and unclear authority; then address your lowest-scoring areas.

Priority 1

Gap / affected AI use: _____

Action and evidence needed: _____

Accountable owner: _____ Target date: _____

Priority 2

Gap / affected AI use: _____

Action and evidence needed: _____

Accountable owner: _____ Target date: _____

Priority 3

Gap / affected AI use: _____

Action and evidence needed: _____

Accountable owner: _____ Target date: _____

Review date: _____ Decision-maker: _____

Useful evidence includes an approved-tool inventory, AI use policy, data rules, approval records, test results, training records, and incident-response procedures.

Build a practical path forward with THBS

THBS helps you turn readiness gaps into clear policies, accountable ownership, human review rules, and practical agent safeguards through AI Governance & Agent Architecture.

Request an AI Governance Consultation

Email: Bizstrategist@Thresholdbusinesssolutions.com

Phone: 726-203-4084

Website: www.thresholdbusinesssolutions.com

Bring your three priorities to the conversation. Keep sensitive client data, passwords, and confidential records out of website forms.

Reference framework & scope

This THBS educational tool is informed by the NIST AI Risk Management Framework 1.0 and its Govern, Map, Measure, and Manage functions. THBS authored the questions and scoring; NIST has not endorsed this checklist. Requirements vary by use, sector, and jurisdiction. Obtain qualified advice for specific legal or regulatory questions.

NIST AI RMF:

<https://www.nist.gov/itl/ai-risk-management-framework>

NIST Playbook:

<https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook>

Version 1.0 | Prepared September 1, 2026

Structure That Sustains Growth | September 2026 | 4