Executive AI Readiness Checklist

A 50-point maturity assessment for enterprise AI programs.

Edition	2026	**Date**	January 07, 2026

Use this checklist to benchmark AI maturity across leadership, governance, technology, operations, and value delivery. Mark each item as True/Implemented for your organization.

Scoring: 0–20 = Early stage | 21–35 = Developing | 36–45 = Operational | 46–50 = Leading

1) Strategy & Leadership (10)

- ☐ We have an executive sponsor accountable for AI outcomes and risk.
- ☐ AI is tied to explicit business objectives (not experimentation alone).
- ☐ We maintain a prioritized portfolio of AI initiatives with owners and milestones.
- ☐ We have defined where AI is allowed, prohibited, and restricted.
- ☐ We have a budget model for AI initiatives (build, buy, operate).
- ☐ We have KPIs that measure both value and risk for AI systems.
- ☐ We communicate AI strategy internally in plain language (what, why, how).
- ☐ We have a policy for employee use of consumer AI tools (e.g., chat assistants).
- ☐ Our board / leadership reviews AI risk and value at a defined cadence.
- ☐ We maintain a process for retiring AI systems that no longer meet requirements.

2) Governance & Risk (10)

- ☐ We classify AI systems by impact and apply tiered controls accordingly.
- ☐ We require documentation for AI systems (purpose, data, limitations, owners).
- ☐ We have an approval workflow for high-impact AI use cases.
- ☐ We perform privacy reviews for AI systems using personal or sensitive data.
- ☐ We conduct security reviews for AI vendors and internally built AI systems.
- ☐ We have a process to detect, triage, and remediate AI incidents.
- ☐ We have guardrails for human oversight in high-risk decisions.
- ☐ We test for bias and harmful outputs appropriate to use-case context.
- ☐ We track third-party model updates and monitor resulting behavioral changes.
- ☐ We have audit trails for key AI decisions, approvals, and deployments.

3) Data & Technology (10)

- ☐ We know which datasets are used for which AI systems (lineage).
- ☐ We enforce role-based access control for data and model endpoints.
- ☐ We have data quality checks and monitoring for critical datasets.
- ☐ We have a standard approach for model evaluation and benchmarking.
- ☐ We run red-team or adversarial testing for important AI systems.
- ☐ We monitor model drift and performance degradation in production.
- ☐ We have controls to prevent sensitive data leakage (prompts, logs, outputs).
- ☐ We have an architecture standard for integrating AI safely into products.
- ☐ We have clear environments (dev/test/prod) and change management controls.
- ☐ We have an inventory of AI systems, models, tools, and vendors in use.

4) People & Operating Model (10)

- ☐ We have a cross-functional AI council or steering group.
- ☐ We have clear roles for product, engineering, legal, risk, and data governance.
- ☐ We have training for staff on safe AI use and escalation paths.
- ☐ We have guidelines for prompt design, data handling, and disclosure.
- ☐ We have a defined process for onboarding new AI vendors/tools.
- ☐ We have a repeatable delivery process (intake → build → approve → deploy → monitor).

- ☐ We staff or contract the capabilities needed (ML/LLM, security, compliance, change).
- ☐ We can respond quickly to AI incidents (who, when, how).
- ☐ We have a communication plan for external stakeholders if AI incidents occur.
- ☐ We review and update policies as AI regulations and tools evolve.

5) Value & Delivery (10)

- ☐ We can quantify expected benefits for AI initiatives (cost, revenue, risk).
- ☐ We use a consistent ROI model including assumptions and sensitivity.
- ☐ We measure realized value after deployment and compare to projections.
- ☐ We have a framework to stop/iterate initiatives that are not delivering.
- ☐ We have a playbook for scaling successful pilots into production.
- ☐ We track adoption and user behavior to ensure AI features are actually used.
- ☐ We capture operational cost of AI (inference, data, licenses, support) over time.
- ☐ We define SLAs and reliability expectations for AI systems.
- ☐ We include fairness, safety, and security criteria in go/no-go decisions.
- ☐ We maintain a backlog of improvements based on monitoring and feedback.

Scoring guidance

0–20: Early stage — foundational policies and inventory needed.
21–35: Developing — controls exist but are not consistent across teams.
36–45: Operational — governance is embedded and monitored.
46–50: Leading — mature controls, reporting, and continuous improvement.

If you'd like an independent executive assessment and roadmap, contact: advisory@cichocki.com