

AI Readiness Assessment Toolkit

A structured executive toolkit for determining whether the enterprise is ready to adopt, govern, secure and scale artificial intelligence.

STRATEGY	DATA	TECHNOLOGY	GOVERNANCE	PEOPLE	RISK
Value	Foundation	Architecture	Control	Capability	Confidence

EXECUTIVE PURPOSE

Replace enthusiasm-based AI adoption with an evidence-based readiness view, prioritized gaps and a practical roadmap for responsible scale.

YAKAMICHI PERSPECTIVE

AI readiness is not measured by how many pilots exist. It is measured by whether the organization can turn AI into repeatable value without losing control of risk.

Contents & Assessment Method

SECTION	CONTENT
01	Readiness Mandate & Assessment Scope
02	Strategy & Value Readiness
03	Data Readiness
04	Technology & Architecture Readiness
05	Governance & Responsible AI Readiness
06	Security, Privacy & Compliance Readiness
07	People, Skills & Operating Model Readiness
08	Use-Case Portfolio & Prioritization
09	Scoring, Heatmap & Executive Findings
10	180-Day AI Readiness Roadmap
A-F	Questionnaire, Scoring Sheet, Use-Case Canvas, Heatmap, Executive Report & Checklist

Six Readiness Dimensions

- Strategy: clarity of business outcomes, sponsorship and investment logic.
- Data: availability, quality, ownership, permissions and lifecycle controls.
- Technology: platforms, integration, identity, observability and deployment capability.
- Governance: decision rights, inventory, policy, risk tiering and human oversight.
- People: leadership literacy, product ownership, technical skills and change capability.
- Risk: cybersecurity, privacy, legal, third-party and operational assurance.

ASSESSMENT RULE

Score evidence, not aspiration. A planned control or future hire should not receive the same readiness score as a capability that is operating and demonstrable.

Readiness Mandate & Assessment Scope

The assessment should establish a common baseline before major AI investment, enterprise scaling or transformation. Scope can be enterprise-wide or focused on a business unit, platform or strategic use-case portfolio.

QUESTION	EVIDENCE
Why AI now?	Strategic objective, business case and executive sponsor
Where will AI be used?	Functions, processes, customers and decisions
What consequence could failure create?	Operational, legal, financial, people and reputation impact
What already exists?	Pilots, embedded AI, vendors, models and shadow use
Who owns readiness?	Named executive and cross-functional assessment team

- Define assessment boundary and time horizon.
- Identify executive sponsor and decision to be informed.
- Collect existing policies, architecture, data and AI inventories.
- Interview business, data, technology, security, legal, privacy and HR leaders.
- Validate scores with evidence and record material disagreements.

SCOPE PRINCIPLE

Readiness is contextual. An enterprise may be ready for low-risk productivity copilots while unready for autonomous or consequential decision systems.

Strategy & Value Readiness

AREA	READINESS TEST
Strategic alignment	AI priorities connect to explicit enterprise objectives
Executive sponsorship	A senior leader owns outcomes and cross-functional barriers
Value hypothesis	Use cases have measurable benefits, costs and assumptions
Portfolio discipline	Pilots are prioritized rather than accumulated
Funding	Investment includes data, controls, integration, change and monitoring
Scale criteria	Leadership knows what evidence is required to expand or stop

Executive Questions

- Which business outcomes are important enough to justify AI investment?
- Where does AI create an advantage versus ordinary automation or process redesign?
- Which use cases could create material downside if outputs are wrong?
- What evidence will cause us to scale, redesign or stop a pilot?
- Who owns realized value after technical deployment?

VALUE PRINCIPLE

A technically successful model can still be a failed investment. Readiness includes the ability to redesign work, measure outcomes and stop low-value experimentation.

Data Readiness

AI performance inherits the strengths and weaknesses of enterprise data. Readiness requires more than volume: data must be usable, lawful, sufficiently trustworthy and governed for the intended purpose.

AREA	EVIDENCE
Ownership	Named data owners and stewardship
Quality	Defined quality measures for critical datasets
Access	Authorized, auditable access appropriate to purpose
Classification	Sensitive and regulated data identified
Lineage	Important sources and transformations understood
Permissions	Use is compatible with privacy, contract and licensing terms
Lifecycle	Retention, deletion and archival rules operating

Readiness Red Flags

- Critical datasets have no accountable owner.
- Teams cannot explain whether sensitive data may be used with a proposed AI service.
- Training or retrieval data is duplicated across uncontrolled locations.
- Quality issues are known but not measured.
- Data access depends on manual exceptions or shared credentials.
- No process exists to remove obsolete or prohibited data from AI workflows.

DATA PRINCIPLE

The question is not 'Do we have data?' It is 'Do we have the right to use sufficiently trustworthy data for this specific AI purpose?'

Technology & Architecture Readiness

CAPABILITY	READINESS EVIDENCE
Platform strategy	Approved patterns for build, buy and managed AI services
Integration	Secure APIs, workflow integration and environment separation
Identity	User, service and privileged access controls
Model lifecycle	Versioning, testing, release and rollback practices
Observability	Logs, performance monitoring, cost and usage visibility
Resilience	Fallback, continuity and provider outage considerations
Scalability	Capacity and architecture can support expected adoption

Architecture Decisions

- Which capabilities should be purchased versus developed?
- Where may sensitive data be processed and stored?
- How will models, prompts and configurations be version-controlled?
- How are AI agents or tools constrained when they can take actions?
- What happens if the model provider changes behavior, terms or availability?
- Can teams monitor cost, performance and security after deployment?

ARCHITECTURE PRINCIPLE

Readiness favors a small number of governed, reusable patterns over a maze of isolated pilots with different security and data assumptions.

Governance & Responsible AI Readiness

CONTROL	READINESS EVIDENCE
Inventory	Material AI systems and use cases are visible
Policy	Acceptable, restricted and prohibited uses defined
Risk tiering	Governance depth increases with consequence
Decision rights	Business, governance and control-function roles are explicit
Human oversight	Review, override and escalation are meaningful
Transparency	Documentation/disclosure expectations are defined
Monitoring	Material change triggers and reassessment rules exist

Maturity Test

- Can an employee tell whether a proposed AI use requires review?
- Can leadership identify all high-impact AI systems and their owners?
- Does approval record residual risk and conditions?
- Are policy exceptions time-bound and visible?
- Can the organization suspend an AI capability when monitoring shows unacceptable behavior?

GOVERNANCE PRINCIPLE

Governance should be usable enough that teams enter the process early. If review is opaque or excessively slow, adoption migrates into the shadows.

Security, Privacy & Compliance Readiness

DOMAIN	READINESS TEST
Cybersecurity	Threat modeling, access, secrets, APIs and adversarial testing appropriate to risk
Privacy	Purpose, minimization, sensitive data, retention and rights addressed
Legal	Contracts, intellectual property, records and sector obligations reviewed
Third party	Provider security, data use, subprocessors and exit understood
Incident response	AI-specific incidents connect to enterprise response
Assurance	Evidence exists that required controls operate, not only that policy requires them

Minimum Questions Before Scale

- Can confidential information enter the model, and under what conditions?
- Does the provider retain or use organizational data for training?
- How are prompt injection, tool abuse or unauthorized actions constrained?
- What legal or regulatory obligations change because AI is involved?
- Who can contain the system and preserve evidence after a material incident?

RISK PRINCIPLE

Readiness is not zero risk. It is the ability to identify material risk, apply proportionate controls and assign residual risk to an authorized owner.

People, Skills & Operating Model Readiness

CAPABILITY	READINESS EVIDENCE
Executive literacy	Leaders understand AI opportunity, limitations and accountability
Business ownership	Product/process owners remain accountable for outcomes
Technical skills	Data, engineering, architecture and model expertise available
Control skills	Security, privacy, legal and risk teams understand AI-specific issues
Workforce adoption	Users receive practical guidance and role-based training
Change management	Processes, roles, incentives and measures adapt with technology

Capability Gaps

- AI expertise is concentrated in one technical team with weak business ownership.
- Executives expect technology teams to own business outcomes.
- Staff use public AI tools because approved alternatives are unavailable.
- Control functions review AI only at procurement or launch.
- Training teaches features but not data handling, verification or escalation.
- No workforce plan addresses how roles and processes will change.

PEOPLE PRINCIPLE

AI transformation is work transformation. Readiness depends on whether people can redesign, supervise and improve the process around the technology.

Use-Case Portfolio & Prioritization

A readiness assessment should end with choices. Use cases can be evaluated across value, feasibility, readiness and risk so scarce attention goes to initiatives with a credible path to impact.

FACTOR	QUESTIONS
Value	How large and measurable is the expected outcome?
Feasibility	Are data, integration and technical requirements achievable?
Readiness	Do governance, skills and operational controls exist?
Risk	What consequence could error, misuse or failure create?
Time to value	How quickly can evidence be generated?
Reusability	Does the capability create a foundation for other use cases?

Portfolio Categories

- Accelerate** High value, strong readiness, manageable risk.
- Prepare** High value but foundational gaps must be closed first.
- Experiment** Uncertain value; use controlled pilot to generate evidence.
- Defer** Dependencies or economics are not yet favorable.
- Do Not Pursue** Risk, legality or strategic fit is unacceptable.

PORTFOLIO PRINCIPLE

Do not confuse novelty with priority. The best first use cases often combine visible value, available data, limited consequence and reusable foundations.

Scoring, Heatmap & Executive Findings

Use a consistent scoring model to create comparability without pretending that readiness is mathematically precise. Scores should be supported by evidence and accompanied by narrative findings.

SCORE	MATURITY	DESCRIPTION
1	Ad Hoc	Little evidence; capability depends on individuals or informal practice
2	Emerging	Some defined practice; inconsistent coverage or evidence
3	Managed	Repeatable process with accountable ownership and operating evidence
4	Adaptive	Measured, integrated and continuously improved capability

Executive Output

- Overall readiness profile by dimension.
- Top strengths that can be leveraged immediately.
- Critical gaps that block high-value AI use cases.
- High-risk conditions requiring executive decision.
- Prioritized use-case portfolio.
- 90/180-day actions, owners, dependencies and investment implications.

SCORING PRINCIPLE

Averages can hide a critical weakness. A strong overall score should not override a material security, legal, data or governance blocker for a specific high-impact use case.

180-Day AI Readiness Roadmap

WINDOW	PRIORITY	DELIVERABLES
0–30 Days	Baseline	Scope, sponsor, inventory, interviews, initial scoring and priority use cases
31–60 Days	Foundations	Data ownership, approved technology patterns, interim AI policy and risk tiers
61–90 Days	Operating model	Governance workflow, decision rights, security/privacy review and training
91–120 Days	Controlled pilots	Launch selected use cases with measures, monitoring and human oversight
121–150 Days	Close scale blockers	Remediate critical data, integration, supplier and control gaps
151–180 Days	Scale decision	Re-score readiness, validate value, approve portfolio and investment roadmap

Day-180 Decision

- Which AI capabilities are ready for enterprise scale?
- Which use cases remain constrained and why?
- Which foundational investments unlock multiple priorities?
- Which risks require executive acceptance or redesign?
- What should the next 12-month AI portfolio contain?

ROADMAP PRINCIPLE

The assessment is not complete when the score is published. It is complete when leadership knows what to accelerate, what to fix, what to defer and who owns the next move.

AI Readiness Questionnaire

DIMENSION	ASSESSMENT QUESTIONS
Strategy	Are AI priorities tied to measurable objectives? Is sponsorship clear? Are scale/stop criteria defined?
Data	Are critical datasets owned, usable, lawful, sufficiently high quality and accessible?
Technology	Are approved AI patterns, secure integration, identity, monitoring and resilience available?
Governance	Are inventory, policy, risk tiers, decision rights and human oversight operating?
People	Do leaders, business owners, technical teams and control functions have appropriate capability?
Risk	Are cyber, privacy, legal, third-party, incident and assurance processes AI-ready?

For each question, record score 1–4, evidence, owner, gap, action and due date.

Readiness Scoring Sheet

DIMENSION	SCORE 1-4	WEIGHT	WEIGHTED	KEY EVIDENCE / GAP
Strategy	—	—%	—	_____
Data	—	—%	—	_____
Technology	—	—%	—	_____
Governance	—	—%	—	_____
People	—	—%	—	_____
Risk	—	—%	—	_____
TOTAL		100%	—	

Weights may vary by assessment purpose. Do not use weighting to dilute a mandatory legal, security or safety requirement.

AI Use-Case Prioritization Canvas

FIELD	RECORD
Use case	_____
Business owner	_____
Outcome / KPI	_____
Value score	1-4 + evidence
Feasibility score	1-4 + evidence
Readiness score	1-4 + evidence
Risk tier	1-4 + rationale
Time to evidence	_____
Dependencies	Data / tech / people / supplier
Portfolio decision	Accelerate / Prepare / Experiment / Defer / Do Not Pursue

Executive Readiness Heatmap

CAPABILITY	STRATEGY	DATA	TECH	GOVERNANCE	PEOPLE	RISK
Current	—	—	—	—	—	—
Target 6 months	—	—	—	—	—	—
Target 12 months	—	—	—	—	—	—

Top Five Gaps

1.
2.
3.
4.
5.

Top Five Enablers

1.
2.
3.
4.
5.

Executive AI Readiness Report Template

EXECUTIVE JUDGMENT

Overall readiness and what leadership should decide.

READINESS PROFILE

Scores by six dimensions, with evidence and material caveats.

BUSINESS OPPORTUNITY

Priority use cases and expected outcomes.

CRITICAL BLOCKERS

Gaps that prevent safe or effective scale.

RISK POSITION

Material residual risks and decisions required.

180-DAY PLAN

Actions, owners, investment and milestones.

12-MONTH OUTLOOK

Capabilities expected to become scalable and remaining dependencies.

Readiness Maturity Model & Executive Checklist

LEVEL	CHARACTERISTICS	EXECUTIVE MEANING
1 — Ad Hoc	Isolated pilots, unclear ownership, fragmented data/control	Experimentation exceeds readiness
2 — Emerging	Foundations forming; inconsistent process and skills	Selective pilots are appropriate
3 — Managed	Repeatable governance, data, architecture and operating model	Responsible scale is achievable
4 — Adaptive	Measured portfolio, reusable platforms and continuous assurance	AI becomes an enterprise capability

Executive Checklist

- ☐ AI objectives tied to enterprise strategy
- ☐ Executive sponsor and business owners named
- ☐ Material AI use inventoried
- ☐ Critical data ownership and permissions understood
- ☐ Approved technology and integration patterns available
- ☐ AI governance and risk tiers operating
- ☐ Security/privacy/legal reviews integrated
- ☐ Workforce skills and change plan established
- ☐ Priority use cases scored and sequenced
- ☐ 180-day remediation and scale roadmap approved

Yakamichi Perspective

Readiness creates the bridge between AI ambition and AI performance. Organizations that understand their foundations can invest deliberately, scale the right use cases and avoid paying twice for capabilities they should have built first.

REQUEST A CONFIDENTIAL CONSULTATION

United States: +1 202 413 3763 | Maryland, USA
Nigeria: +234 811 095 0651 | Abuja, Nigeria

YAKAMICHI • Artificial Intelligence • Cybersecurity • Counter-Surveillance • Corporate Risk Intelligence