CTRL THE FUTURE LLC

AI GOVERNANCE READINESS CHECKLIST

A practical self-review for responsible AI oversight, risk management, lifecycle controls, and organizational accountability

Purpose: This checklist helps organizations review foundational AI governance and risk-management practices. It is informed by the NIST AI Risk Management Framework (AI RMF) concepts of GOVERN, MAP, MEASURE, and MANAGE, while remaining a practical organizational readiness resource. It is not a certification, legal determination, or substitute for use-case-specific AI risk analysis.

Organization: _____

Completed by: _____

Date: _____

How to Use This Checklist

Review each statement with appropriate business, technology, security, privacy, legal/compliance, data, and operational stakeholders. Select the response that best reflects current practice and document evidence, ownership, or follow-up actions.

ESTABLISHED	PARTIAL	NOT ESTABLISHED	N/A
Operating consistently	Some elements exist	Absent or unknown	Not applicable

1. AI Governance & Accountability

AI governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Executive or senior leadership accountability for AI governance and risk is defined.	■	■	■	■	
AI-related roles, responsibilities, decision rights, and escalation paths are documented.	■	■	■	■	
Policies or standards establish expectations for responsible acquisition, development, deployment, and use of AI.	■	■	■	■	
AI risk management is integrated with relevant enterprise risk, cybersecurity, privacy, compliance, and technology governance processes.	■	■	■	■	
AI governance practices are periodically reviewed as technologies, risks, laws, and organizational uses evolve.	■	■	■	■	

2. AI Inventory & Use-Case Oversight

AI governance readiness statement	Established	Partial	Not Est.	N/A	Notes
The organization maintains an inventory of AI systems, AI-enabled products, and significant generative AI uses.	■	■	■	■	
Each material AI use case has an identified business owner and intended purpose.	■	■	■	■	
AI systems are categorized or prioritized based on potential impact, sensitivity, and risk.	■	■	■	■	
Unapproved or unmanaged AI use is addressed through policy, awareness, technical controls, or other governance mechanisms.	■	■	■	■	
Third-party and embedded AI capabilities are included in inventory and governance processes where relevant.	■	■	■	■	

3. Context, Impact & Stakeholder Mapping

AI governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Intended users, affected individuals or groups, business context, and foreseeable uses of material AI systems are identified.	■	■	■	■	
Potential benefits, harms, misuse, and unintended consequences are considered before deployment.	■	■	■	■	
Human-AI roles and decision responsibilities are documented for material use cases.	■	■	■	■	
Relevant internal and external stakeholder perspectives are considered when evaluating significant AI impacts.	■	■	■	■	
Context and impact assumptions are revisited when the AI system or its operating environment changes.	■	■	■	■	

4. Data Governance & Privacy

AI governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Data used with AI systems has defined ownership, permitted use, quality expectations, and appropriate access controls.	■	■	■	■	
Privacy and confidentiality risks are evaluated before sensitive or personal information is used with AI.	■	■	■	■	
Data provenance, limitations, representativeness, and quality are considered where relevant to system outcomes.	■	■	■	■	
Policies address the entry of confidential, proprietary, regulated, or personal data into external AI services.	■	■	■	■	
Retention, deletion, sharing, and secondary-use expectations are defined for AI-related data when applicable.	■	■	■	■	

5. Security, Resilience & Misuse

AI governance readiness statement	Established	Partial	Not Est.	N/A	Notes
AI systems are included in relevant cybersecurity and secure-configuration practices.	■	■	■	■	
Threats such as unauthorized access, data leakage, malicious inputs, model or prompt abuse, and unsafe integrations are considered.	■	■	■	■	
Access to AI administration, models, sensitive data, and high-impact capabilities is restricted appropriately.	■	■	■	■	
Security monitoring and incident-response processes include material AI-related events where applicable.	■	■	■	■	
Resilience, fallback, recovery, and safe shutdown or suspension options are considered for important AI-supported processes.	■	■	■	■	

6. Testing, Measurement & Validation

AI governance readiness statement	Established	Partial	Not Est.	N/A	Notes
AI systems are evaluated before deployment against defined performance, risk, and trustworthiness criteria appropriate to the use case.	■	■	■	■	
Testing considers limitations, error conditions, uncertainty, and reasonably foreseeable misuse.	■	■	■	■	
Metrics and evaluation methods are documented sufficiently to support repeatability and oversight.	■	■	■	■	
Material AI systems are monitored and reevaluated after deployment when performance, context, data, or risk changes.	■	■	■	■	
Independent or appropriately separated review is considered for higher-risk AI use cases.	■	■	■	■	

7. Human Oversight, Transparency & Accountability

AI governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Human review or intervention is defined where AI outputs could materially affect people, operations, rights, safety, or significant decisions.	■	■	■	■	
Users understand when and how AI is being used in relevant organizational processes.	■	■	■	■	
AI-generated outputs are subject to appropriate verification before consequential use.	■	■	■	■	
Documentation supports traceability of important AI decisions, approvals, changes, and risk treatments.	■	■	■	■	
Processes exist to escalate, challenge, override, or stop AI-supported decisions or operations when appropriate.	■	■	■	■	

8. Third-Party & Vendor AI Risk

AI governance readiness statement	Established	Partial	Not Est.	N/A	Notes
AI vendors and externally provided AI capabilities undergo risk-based review before material use.	■	■	■	■	
Vendor due diligence considers security, privacy, data handling, performance, transparency, contractual, and continuity risks as appropriate.	■	■	■	■	
Contracts or agreements address relevant AI-related responsibilities, data use, confidentiality, incident notification, and service expectations.	■	■	■	■	
Material changes to third-party AI services are monitored when they could affect organizational risk.	■	■	■	■	
Exit, replacement, data-return/deletion, and continuity considerations are addressed for important AI vendors.	■	■	■	■	

9. Generative AI & Responsible Use

AI governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Acceptable-use expectations are defined for generative AI tools used by personnel.	■	■	■	■	
Users are trained to verify AI-generated content rather than assuming outputs are accurate or authoritative.	■	■	■	■	
Processes address risks such as fabricated content, harmful outputs, intellectual-property concerns, confidential-data exposure, and overreliance.	■	■	■	■	
High-impact uses of generative AI receive additional review before deployment or operational reliance.	■	■	■	■	
Generative AI incidents, recurring errors, and emerging risks are captured and used to improve governance.	■	■	■	■	

10. Risk Treatment & Continuous Improvement

AI governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Identified AI risks are documented, prioritized, assigned owners, and treated according to organizational risk tolerance.	■	■	■	■	
Decisions to mitigate, transfer, avoid, accept, pause, or discontinue AI use are documented when material.	■	■	■	■	
AI incidents, near misses, complaints, monitoring results, and lessons learned inform improvement activities.	■	■	■	■	
Leadership receives meaningful information about material AI risks, performance, and remediation progress.	■	■	■	■	
The organization maintains a roadmap for strengthening AI governance as adoption and risk evolve.	■	■	■	■	

AI Governance Readiness Summary

Use this page to identify governance areas that warrant priority attention. Readiness results should be interpreted in the context of each AI use case, affected stakeholders, applicable requirements, organizational risk tolerance, and the potential magnitude of impact.

Priority Area	Gap / Observation	Owner	Target Date
1.			
2.			
3.			
4.			
5.			

Suggested Next Steps

1. Inventory material AI systems and assign accountable business and risk owners.
2. Prioritize Not Established and Partial items for higher-impact AI use cases first.
3. Establish minimum review requirements for data, security, privacy, human oversight, testing, vendors, and responsible use.
4. Document risk decisions and monitor deployed AI systems for performance changes, incidents, misuse, and emerging risks.
5. Reassess AI governance periodically as organizational adoption, technology, regulation, and risk evolve.

Need help building practical AI governance?
CTRL The Future LLC can help organizations inventory AI use, establish governance structures, assess AI risk, develop responsible-use policies, strengthen oversight, and build an actionable AI governance roadmap.

Framework note: This resource is informed by NIST AI RMF 1.0 and related NIST guidance. NIST describes the AI RMF as voluntary and notes that AI RMF 1.0 is being revised; organizations should monitor authoritative guidance for updates.

Disclaimer: This checklist is for general informational and readiness purposes only. It is not legal advice, certification, a formal audit, or a determination that an AI system is safe, compliant, unbiased, or trustworthy. Assessment should be tailored to the specific AI system, context, stakeholders, and applicable requirements.