

MUZAMANI

INTERNAL AUDIT AI READINESS CHECKLIST

A governance, risk and assurance tool for evaluating organisational readiness to adopt Artificial Intelligence

Purpose	Identify practical strengths, gaps and priority actions before or during the use of AI.
Intended users	Internal audit leaders, risk and compliance teams, executives, audit committees and organisations adopting AI.
Version	1.1 — Revised 10 October 2026
Prepared by	Muzamani Services (Pty) Ltd

Practical self-assessment • Indicative scoring • Action-focused

1. How to use this checklist

Use this checklist to assess whether the organisation has governance, controls, skills and assurance arrangements needed to use artificial intelligence (AI) responsibly. It can be used before adoption, during a pilot, or to review an existing AI-enabled process.

- Complete the checklist through discussion with relevant business, IT, information security, privacy, legal, risk, procurement and internal audit representatives.
- Base answers on evidence where possible, not only on policies or management assurances.
- For each question, select one response: Yes = 2; Partial = 1; No = 0. Select N/A only where the question genuinely does not apply and record a short reason.
- For small organisations, apply the questions proportionately. A control may be delivered by an owner, service provider or group function, but responsibility and oversight should still be clear.
- Treat the result as a diagnostic indicator, not a certification or guarantee that AI is safe, lawful or effective.

Scoring options

Response	Score	Guidance
Yes	2	The control or practice is in place and supported by reasonable evidence.
Partial	1	The control exists in part, is inconsistent, or needs improvement.
No	0	The control is absent, ineffective or not evidenced.
N/A	Excluded	Not applicable to the organisation or use case; explain why.

Organisation and assessment details

Field	Details
Organisation / business unit	
Country / jurisdiction(s)	
Assessment date	
Assessor(s) and role(s)	
AI systems / use cases in scope	
AI lifecycle stage	☐ Considering ☐ Pilot ☐ In use ☐ Scaling / material change
Key stakeholders consulted	

2. Readiness questions

For each question, mark one response. Use the evidence/notes column to record documents reviewed, examples, control owners or actions needed.

A. Strategy, accountability and proportionality

No.	Readiness question	Yes (2)	Partial (1)	No (0)	N/A	Evidence / notes
01	Has the organisation identified the business objectives and intended benefits for each material AI use case?	☐	☐	☐	☐	
02	Is there a named executive or accountable owner for each material AI system or use case?	☐	☐	☐	☐	
03	Are responsibilities for approving, operating, monitoring and reviewing AI use clearly assigned?	☐	☐	☐	☐	
04	Is there an AI policy or set of documented principles proportionate to the organisation's size and risk exposure?	☐	☐	☐	☐	
05	Are AI use cases assessed and approved before deployment, with a defined route for exceptions?	☐	☐	☐	☐	

06	Does the organisation maintain an inventory of material AI systems, tools, models and business use cases?	☐	☐	☐	☐	
07	Are employees told which AI tools are approved and which uses are prohibited or restricted?	☐	☐	☐	☐	

B. Risk, impact and legal compliance

No.	Readiness question	Yes (2)	Partial (1)	No (0)	N/A	Evidence / notes
08	Are AI-related risks assessed before a system is acquired, developed or materially changed?	☐	☐	☐	☐	
09	Do assessments consider operational, financial, legal, privacy, security, reputational, fairness and human impacts as relevant?	☐	☐	☐	☐	
10	Are higher-risk uses subject to stronger review and approval than low-risk uses?	☐	☐	☐	☐	

11	Are applicable laws, regulatory obligations, contractual commitments and sector requirements identified for each material use case?	☐	☐	☐	☐	
12	Where AI processes personal information, are lawful processing, purpose limitation, data minimisation and other applicable privacy requirements assessed?	☐	☐	☐	☐	
13	Where AI is used to make decisions based solely on automated processing that may have legal or substantial effects on individuals, does the organisation assess compliance with POPIA section 71, including applicable exceptions and safeguards?	☐	☐	☐	☐	
14	Are material AI risks recorded, assigned to owners and tracked until resolved or formally accepted by an authorised person?	☐	☐	☐	☐	

C. Data governance, privacy and confidentiality

No.	Readiness question	Yes (2)	Partial (1)	No (0)	N/A	Evidence / notes
15	Is the source, ownership, quality and permitted use of data for each material AI use case understood?	☐	☐	☐	☐	
16	Are personal, confidential, commercially sensitive and privileged information identified and handled according to approved rules?	☐	☐	☐	☐	
17	Have staff been told what information must not be entered into public or unapproved AI tools?	☐	☐	☐	☐	
18	Are AI provider terms checked for data retention, model training, data sharing, subprocessors, location and deletion arrangements where relevant?	☐	☐	☐	☐	
19	Are data access rights restricted to people and systems that need them?	☐	☐	☐	☐	
20	Are data quality, representativeness, accuracy and known limitations assessed for the intended use?	☐	☐	☐	☐	
21	Are data retention and deletion arrangements defined and monitored where applicable?	☐	☐	☐	☐	

D. Model selection, output quality and human oversight

No.	Readiness question	Yes (2)	Partial (1)	No (0)	N/A	Evidence / notes
22	Has the organisation assessed whether AI is suitable for the task compared with non-AI alternatives?	☐	☐	☐	☐	
23	Are the model or tool's intended purpose, limitations and known failure modes documented?	☐	☐	☐	☐	
24	Are outputs checked for accuracy, relevance, bias, fabricated information and other foreseeable errors before consequential use?	☐	☐	☐	☐	
25	Is a suitably qualified person responsible for reviewing AI outputs where judgement or material consequences are involved?	☐	☐	☐	☐	
26	Can staff challenge, override or escalate AI-generated outputs or recommendations?	☐	☐	☐	☐	
27	Are users informed when AI materially contributes to a decision or output where this is appropriate or required?	☐	☐	☐	☐	
28	Are performance, accuracy and other relevant quality measures defined and reviewed after deployment?	☐	☐	☐	☐	

E. Cybersecurity, access and operational resilience

No.	Readiness question	Yes (2)	Partial (1)	No (0)	N/A	Evidence / notes
29	Have security risks associated with the AI system, its integrations, prompts, data and outputs been assessed?	☐	☐	☐	☐	
30	Are authentication, access control and privileged access appropriate to the risk?	☐	☐	☐	☐	
31	Are AI tools and integrations subject to relevant vulnerability, configuration and change-management controls?	☐	☐	☐	☐	
32	Are safeguards considered for prompt injection, data leakage, malicious inputs, unsafe outputs and misuse where relevant?	☐	☐	☐	☐	
33	Are security events and material AI actions logged where appropriate, with privacy, access and retention controls?	☐	☐	☐	☐	

34	Is there a process to report, investigate and respond to AI-related incidents and harmful outputs?	☐	☐	☐	☐	
35	Can the organisation suspend, roll back or safely disable an AI system if material problems occur?	☐	☐	☐	☐	

F. Third parties, procurement and financial control

No.	Readiness question	Yes (2)	Partial (1)	No (0)	N/A	Evidence / notes
36	Is there an appropriate due-diligence process for AI vendors, platforms, consultants and other third parties?	☐	☐	☐	☐	
37	Are the provider's security, privacy, reliability, performance and support arrangements assessed in proportion to risk?	☐	☐	☐	☐	
38	Do contracts address relevant matters such as data use, confidentiality, incident notification, audit or assurance rights, service levels and exit arrangements?	☐	☐	☐	☐	

39	Are ownership and permitted use of prompts, outputs, training data and other intellectual property considered?	☐	☐	☐	☐	
40	Are AI costs, licences, usage limits and expected benefits monitored against approved budgets or business cases?	☐	☐	☐	☐	
41	Are material supplier dependencies, service interruptions and exit or replacement options considered?	☐	☐	☐	☐	

G. People, skills and responsible use

No.	Readiness question	Yes (2)	Partial (1)	No (0)	N/A	Evidence / notes
42	Have staff who use or oversee AI received role-appropriate guidance or training?	☐	☐	☐	☐	
43	Do relevant decision-makers understand the limitations and risks of the AI systems they rely on?	☐	☐	☐	☐	

44	Are staff expected to verify important AI-generated information rather than accept it uncritically?	☐	☐	☐	☐	
45	Is there a clear way for staff or affected people to raise concerns about AI use or outcomes?	☐	☐	☐	☐	
46	Are accessibility, fairness, discrimination and potential impacts on affected groups considered where relevant?	☐	☐	☐	☐	
47	Are incentives and performance expectations consistent with responsible use rather than unchecked AI adoption?	☐	☐	☐	☐	

H. Monitoring, change and incident management

No.	Readiness question	Yes (2)	Partial (1)	No (0)	N/A	Evidence / notes
48	Are owners assigned to monitor material AI systems after deployment?	☐	☐	☐	☐	
49	Are thresholds defined for errors, performance deterioration, unusual behaviour or other triggers for review?	☐	☐	☐	☐	
50	Are material changes to models, data, prompts, integrations or intended use assessed before implementation where feasible?	☐	☐	☐	☐	
51	Are AI incidents, near misses, complaints and corrective actions recorded and reviewed for lessons?	☐	☐	☐	☐	
52	Are material AI systems periodically reassessed and reapproved when risk, context or requirements change?	☐	☐	☐	☐	

53	Is there a documented process for notifying relevant stakeholders and meeting applicable reporting obligations after an incident?	☐	☐	☐	☐	
----	---	--------------------------	--------------------------	--------------------------	--------------------------	--

I. Internal audit, independent assurance and improvement

No.	Readiness question	Yes (2)	Partial (1)	No (0)	N/A	Evidence / notes
54	Has management identified which AI-related controls require independent assurance based on risk and materiality?	☐	☐	☐	☐	
55	Does the internal audit function understand the organisation's material AI use cases and related risks, or have access to suitable specialist support?	☐	☐	☐	☐	
56	Are AI-related assurance activities included in risk-based audit planning where warranted?	☐	☐	☐	☐	

57	Can internal audit access relevant documentation, system information, personnel and third-party assurance evidence subject to applicable rights and safeguards?	☐	☐	☐	☐	
58	Are assurance findings assigned to accountable management owners, with due dates and follow-up?	☐	☐	☐	☐	
59	Is management responsibility for AI governance and controls kept separate from internal audit's independent assurance role?	☐	☐	☐	☐	
60	Are lessons from assessments, incidents, assurance reviews and changes used to improve the AI control environment?	☐	☐	☐	☐	

3. Scoring and interpretation

The checklist contains 60 questions. The maximum possible score is 120 points if every question applies. N/A responses are excluded from the denominator.

Calculation

Readiness score (%) = Points achieved ÷ Maximum applicable points × 100

Maximum applicable points = Number of applicable questions × 2. Points achieved are the total of Yes (2), Partial (1) and No (0) responses. Do not count N/A responses in either the numerator or denominator.

Indicative maturity bands

Score	Level	Interpretation	Suggested focus
0–19%	Level 1 — Initial / Ad hoc	AI use may be informal, with limited consistent governance or control.	Address urgent legal, privacy, security and accountability gaps; restrict high-risk use until reviewed.
20–39%	Level 2 — Developing	Some practices exist, but coverage and implementation are inconsistent.	Assign owners; document approved use; introduce proportionate risk assessments and staff guidance.
40–59%	Level 3 — Defined	Core policies and controls are documented, though implementation or monitoring may be uneven.	Close implementation gaps; define measures, escalation routes and oversight.
60–79%	Level 4 — Managed	Most key controls appear established and monitored, with targeted improvements needed.	Test whether controls work in practice; strengthen monitoring and independent assurance.
80–100%	Level 5 — Optimised	A comparatively mature approach may be in place, with regular review and improvement.	Validate evidence, address residual risks and continue monitoring as systems and requirements change.

These bands are indicative and have not been externally validated. A high overall score does not guarantee that controls are effective or that a particular AI use is appropriate. Serious gaps in legal compliance, personal information, cybersecurity, consequential decisions, financial exposure or critical operations should be treated as priorities regardless of the total score.

Section summary

Section	Question nos.	Questions	Points achieved	Applicable max.	Score %	Priority / notes
A. Strategy, accountability and proportionality	1–7	7				

B. Risk, impact and legal compliance	8–14	7				
C. Data governance, privacy and confidentiality	15–21	7				
D. Model selection, output quality and human oversight	22–28	7				
E. Cybersecurity, access and operational resilience	29–35	7				
F. Third parties, procurement and financial control	36–41	6				
G. People, skills and responsible use	42–47	6				
H. Monitoring, change and incident management	48–53	6				
I. Internal audit, independent assurance and improvement	54–60	7				

For each section: section score (%) = section points achieved ÷ section maximum applicable points × 100. Use the section results to identify concentrated weaknesses that may be hidden by the overall score.

4. Priority action plan

Record practical actions for the most important gaps. Prioritise by potential harm, legal or regulatory exposure, likelihood, scale of impact and how quickly the risk can be reduced.

Priority / gap	Action required	Accountable owner	Target date	Status / evidence
1				
2				
3				
4				
5				

Suggested priority test

- Could the gap expose personal, confidential or commercially sensitive information?
- Could AI produce or influence a material decision about a person, public service, financial matter or critical operation?
- Could the gap create significant cyber, fraud, procurement, legal, financial or reputational exposure?
- Is the organisation relying on a provider or system without adequate oversight, contractual protection or a practical exit route?
- Is management treating a policy as evidence of effectiveness without testing how the control operates?

Management response

Overall readiness view: ☐ Initial ☐ Developing ☐ Defined ☐ Managed ☐ Optimised

Key risks accepted or escalated:

Next review date:

Management representative / date:

Assessor / date:

5. Reference framework

Use the references below as relevant starting points. Applicability depends on jurisdiction, sector, the organisation's activities and the specific AI use case. This checklist is not a clause-by-clause compliance mapping.

Reference	Potential relevance
ISO/IEC 42001:2023	Artificial intelligence management systems — requirements for establishing, implementing, maintaining and continually improving an AI management system.
ISO/IEC 23894:2023	Information technology — Artificial intelligence — guidance on risk management.
NIST AI Risk Management Framework (AI RMF 1.0, 2023)	Voluntary framework for managing AI risks across the AI lifecycle; check NIST for updates and revision status.
NIST AI 600-1 (2024)	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile.
ISO/IEC 27001:2022	Information security management systems — requirements.
COBIT 2019	Framework for governance and management of enterprise information and technology.
COSO ERM (2017)	Enterprise Risk Management — Integrating with Strategy and Performance.
King V Report on Corporate Governance for South Africa (2025) — Institute of Directors in South Africa (IoDSA) and the King Committee.	Relevant to ethical and effective leadership, governance oversight, risk management, technology and information governance, and assurance, as applicable to the organisation.
Protection of Personal Information Act 4 of 2013 (POPIA)	South African personal information protection requirements; assess section 71 where applicable to solely automated decisions.
Public Finance Management Act 1 of 1999 (PFMA) and Municipal Finance Management Act 56 of 2003 (MFMA)	Relevant public-sector financial management requirements, where applicable.
IIA Global Internal Audit Standards (effective 9 January 2025)	Relevant requirements include internal audit strategy, resources and competencies, quality and performance, and engagement planning and execution. Confirm exact standard references against the official publication.

Important notes

- Confirm current versions, local legal requirements and sector-specific guidance before relying on any reference.
- Do not assume every framework applies to every organisation or every AI use case.
- For legal interpretation, obtain advice from appropriately qualified professionals.
- Internal audit should preserve independence and objectivity; management remains responsible for risk management, controls and AI governance.

Disclaimer

This checklist is a general self-assessment aid prepared by Muzamani Services (Pty) Ltd. It is not legal advice, a formal certification, a technical validation of an AI system, or a substitute for a risk assessment, control testing or specialist review. Results depend on the accuracy and completeness of responses and supporting evidence. Organisations should adapt the checklist to their size, sector, jurisdiction and AI use cases.

© 2026 Muzamani Services (Pty) Ltd. All rights reserved.