



Knowledge Management

14 April 2026

SOUTH AFRICA

- A practical guide to AI governance for businesses



For more insight into our expertise and services

A practical guide to AI governance for businesses

Artificial intelligence (AI) is compressing decision cycles across every professional workflow. In some instances, businesses are deploying AI agents: systems capable of executing tasks and making decisions autonomously, without direct human intervention. This acceleration has consequences for how human judgement is exercised, how accountability operates and how risk accumulates.

To deliver quality outcomes that remain defensible in the face of regulatory, legal and client scrutiny, organisations need governance that is designed to minimise risk without hindering productivity.

Why AI impacts judgment

AI produces outputs that are fast, coherent and superficially logical. These outputs are intentionally engineered to be accepted. In compressed timeframes, people tend to lean on intuitive acceptance rather than deliberate evaluation.

Early studies show that, over time, reliance on AI creates cognitive offloading (the tendency to delegate thinking tasks to external tools rather than performing them oneself): users outsource steps of reasoning and quality assurance to the

tool, and their own critical faculties are engaged later, or not at all. Automation bias, authority signalling and the absence of obvious "friction" encourage users to treat AI results as default answers.

As a result, decisions are made earlier, faster and more frequently, and overlooked errors can compound. This is especially the case when AI agents are deployed and human oversight is further removed from the workflow cycle.

Corporate governance has not kept pace with workflows

Most corporate governance structures were established for human-led processes with natural pauses and clear review points. Where AI is mentioned, it is often framed as a question of permissibility: may employees use AI, and for what categories of work?

While this is necessary, it is insufficient on its own.

The reality is that AI blurs the boundary between drafting, analysis, review and approval. Oversight models that assume "someone will check this later" become unrealistic when outputs are generated and acted upon in near real time. Accountability may still be formally assigned, but it becomes impractical to exercise without redesigned workflows.

As AI workflows outpace governance, the inevitable result is increased risk exposure.



The accountability vacuum

Despite the changes in how work is performed, South African businesses are largely still subject to the same legal, regulatory and commercial obligations.

Corporate governance

In South Africa, under the Companies Act 71 of 2008, duties of directors and prescribed officers continue to require the exercise of care, skill and diligence, regardless of whether AI was involved in the work. The King V Code (King V), effective 1 January 2026, recommends that governing bodies provide strategic direction and be accountable for the ethical and compliant acquisition, development and use of technology. For AI, this includes ensuring clear accountability for decisions and outcomes, with human oversight proportionate to risk.

King V emphasises assessing risks from emerging technologies to align with the organisation's risk appetite. It also calls for periodic assurance on the effectiveness, compliance and ethics of technology deployment, ensuring that governance outcomes like ethical culture, performance and prudent control are achieved.

A board that implements structured AI oversight and regular assurance reviews can demonstrate compliance with King V principles and reduce liability exposure if outcomes are later questioned.

Data privacy

The Protection of Personal Information Act 4 of 2013 (POPIA) continues to maintain accountability for processing decisions, data quality and security safeguards. It also explicitly prohibits making significant decisions about a person (like credit card applications) based solely on automated processing, unless a human can review it or a contract allows for it.

In this instance, effective governance requires ensuring that neither data privacy nor AI use are considered in isolation. Ensuring that policies around handling personal information are clear and training staff on the implications of AI use under POPIA are vital to minimising risk.

Labour concerns

AI tools trained on biased data can perpetuate discrimination based on race, gender or other grounds prohibited under the Employment Equity Act 55 of 1998 (EEA), leading to legal liability for employers. Key considerations focus on mitigating algorithmic bias in HR processes like recruitment and performance evaluation.

This risk is mitigated through taking proactive steps. For example, a company auditing its AI tools for bias and documenting corrective actions will be in a stronger position to defend against EEA discrimination claims and demonstrate fair labour practices.

Viewed as a whole, even in the absence of AI-specific laws and regulations, it is expected that clients and regulators will look to human decision-makers and the organisations that employ them, not to technology vendors or AI models, when outcomes are questioned.

Considerations for AI governance

From a practical perspective, effective AI governance may need to move from abstract permissibility around AI use to concrete workflow design. Where friction can be reduced before time pressures set in, businesses are better positioned to make the right behaviour the easiest behaviour in unpredictable circumstances.

This involves an exercise in judgement, which cannot be achieved by templates alone. Risk profiles, error costs, latency tolerance, data contexts, client commitments and regulatory exposures vary materially by function, product and jurisdiction. One-size-fits-all controls have the potential to slow work unnecessarily or leave critical gaps.

Knowledge Management

SOUTH AFRICA

A practical roadmap

Strong governance processes are those that are developed with the intention of being coherent to auditors, regulators and clients, while simultaneously servicing the needs of businesses.

This journey begins with mapping AI-assisted workflows by business outcome, risk profile and required speed. It includes identifying how people actually use tools and redesigning the highest risk workflows so that the requirements for responsible, defensible decision-making are explicit and embedded.

Getting started can feel overwhelming, but these are some of the steps businesses can take to pave the way for a more comprehensive framework:

1. **Draft a clear internal policy** outlining acceptable uses of AI tools (such as ChatGPT, Claude, Copilot, etc.) within the organisation. This should address what types of data may or may not be input into AI systems, confidentiality and data protection, the human review process, and disclosure obligations.
2. **Document all AI tools currently in use** across the business, capturing the tool name and vendor, the business function it supports, what data it processes, how data is used and stored, and who is responsible for oversight.

3. **Implement basic training and awareness** for staff on the capabilities and limitations of generative AI, risks of use and expectations for responsible use. Sessions can be conducted in person or even supported by eLearning.
4. **Designate a person or working group to oversee AI governance.** This person or group should be responsible for reviewing new AI tool requests, monitoring regulatory developments and updating policies as needed.

Businesses that choose a future-focused approach invest both in tools and process. This ensures that increased efficiency does not come with an increase in risk, and that minimising risk does not hinder efficiency. Like successful AI deployment, designing AI governance processes that work may require businesses to engage experts, but the investment is intended to yield dividends in the longer term.

When governance is built at the workflow level and accountability is designed into how people and systems interact, teams can leverage AI to move faster with confidence. Businesses can demonstrate compliance if required to do so and can trust that decisions are consistent and explainable. This ensures that efficiency and compliance are proportionate, sustainable, and designed for commercial success.

Safee-Naaz Siddiqi



BBBEE STATUS: LEVEL ONE CONTRIBUTOR

Our BBBEE verification is one of several components of our transformation strategy and we continue to seek ways of improving it in a meaningful manner.

PLEASE NOTE

This information is published for general information purposes and is not intended to constitute legal advice. Specialist legal advice should always be sought in relation to any particular situation. Cliffe Dekker Hofmeyr will accept no responsibility for any actions taken or not taken on the basis of this publication.

JOHANNESBURG

1 Protea Place, Sandton, Johannesburg, 2196. Private Bag X40, Benmore, 2010, South Africa.
Dx 154 Randburg and Dx 42 Johannesburg.
T +27 (0)11 562 1000 F +27 (0)11 562 1111 E jhb@cdhlegal.com

CAPE TOWN

11 Buitengracht Street, Cape Town, 8001. PO Box 695, Cape Town, 8000, South Africa. Dx 5 Cape Town.
T +27 (0)21 481 6300 F +27 (0)21 481 6388 E ctn@cdhlegal.com

NAIROBI

Merchant Square, 3rd floor, Block D, Riverside Drive, Nairobi, Kenya. P.O. Box 22602-00505, Nairobi, Kenya.
T +254 731 086 649 | +254 204 409 918 | +254 710 560 114
E cdhkenya@cdhlegal.com

ONGWEDIVA

Shop No A7, Oshana Regional Mall, Ongwediva, Namibia.
T +264 (0) 81 287 8330 E cdhnamibia@cdhlegal.com

STELLENBOSCH

14 Louw Street, Stellenbosch Central, Stellenbosch, 7600.
T +27 (0)21 481 6400 E cdhstellenbosch@cdhlegal.com

WINDHOEK

2nd Floor, 4@Steps - East Tower, Hilltop Estate, Kleine Kuppe, Windhoek.
PO Box 97115, Maerua Mall, Windhoek, Namibia, 10020
T +264 833 730 100 E cdhnamibia@cdhlegal.com

©2026 15713/APR

