metrica360°

measure | analyze | transform



Assuring AI Risk for Boards: The Metrica360 AI Governance Model

Four themes. Four questions. Can your board prove its AI risk is under control?

1	**DIRECT** Set the mandate	What have we committed to, and what must we obey in every market?
2	**FRAME** Build the structure	Which standard do we run, and can you show every AI use case?
3	**CONTROL** Manage risk in practice	Was risk assessed before go-live, and when was it last tested?
4	**OWN** Take accountability	Who is accountable, and what does the board see each quarter?

In one quarter: a live AI inventory, an approved risk appetite, obligations mapped across Ghana, the AU, EU, US and China, and a quarterly board risk pack.

Book a board briefing

Afeti Cudjoe, Strategy and Technology Consultant, Accra

info@metrica360group.com

www.metrica360group.com

INSIGHTS

Assuring AI Risk: The Metrica360 AI Governance Model for Boards

Authored by Afeti Cudjoe · 9 October 2026 · Technology Risk

Everyone is talking about AI risk, but how do boards obtain real assurance?

Most organisations rely on a static policy and an oversight committee, an approach that leaves critical governance gaps where risk thrives. Today, AI drives credit decisions, hiring, fraud detection, customer service, software delivery and healthcare. Meanwhile, global regulators across four continents are moving at starkly different speeds, frequently shifting course within months of taking action. Directors, however, remain fully accountable.

The vital question for a board is no longer "Do we have an AI policy?" but rather "Can management demonstrate, theme by theme, that every AI risk is identified, controlled, tested and owned?"

Metrica360 structures board-level AI governance around four actionable themes: **Direct**, **Frame**, **Control** and **Own**. Each translates into a single core question for management, allowing a board committee to evaluate its entire AI exposure through just four targeted inquiries. The test is straightforward: every AI risk must fall within at least one theme. Any risk that fits none represents a governance gap that belongs squarely on the board's agenda.

The model draws on recognised frameworks, including the ISO/IEC and NIST AI Risk Management Frameworks, to turn governance principles into practical controls, clear accountability and demonstrable assurance across the whole organisation. The Metrica360 AI Governance Model, ISO standards and NIST frameworks help organisations structure and demonstrate their approach to AI governance and risk management. They are not laws, and adopting a framework or obtaining certification does not, in itself, guarantee legal compliance or prove that every AI system is safe.

This regulatory review focuses on five key jurisdictions: Ghana, the African Union, the European Union, the United States and China.

AI regulation is evolving, but not uniformly. The EU has adjusted timelines for high-risk AI requirements. In the US, federal policy is moving towards a unified national framework, while states continue to advance their own AI laws, and Colorado revised its AI law before it took effect. The African Union is developing a continental AI framework. Ghana has launched its National AI Strategy, but a national strategy is not comprehensive, binding AI legislation.

The message for boards: regulation will evolve. Accountability cannot wait.

Direct: Set the Mandate

Direct defines what the organisation stands for and what regulators expect across its footprint.

The board's question: What have we committed to regarding AI, and what are our legal obligations in every market we touch?

Three structural elements must be in place:

- **Principles and policy.** Core values and an internal AI policy anchored in global standards, such as the OECD AI Principles, UNESCO Recommendations, G7 Hiroshima Code of Conduct and the Council of Europe AI Convention. The board must formally approve this policy and explicitly define its AI risk appetite.
- **Binding law.** A live register of hard legal obligations organised by jurisdiction. Key compliance benchmarks include the EU AI Act, China's generative AI and synthetic content labelling rules, US state legislation (e.g., Colorado's revised AI regime and Texas's TRAIGA), alongside emerging African frameworks like Ghana's draft Emerging Technologies Bill and the African Union (AU) model law.
- **Soft law and governance guidance.** Non-binding regimes that establish supervisory expectations, including the AU Continental AI Strategy, Ghana's National AI Strategy and US federal executive policies. When incidents occur, courts and regulators routinely use these frameworks as the benchmark for reasonable care.

Typical gaps: *Policies disconnected from decision rights and risk limits; compliance mapped only for headquarters while systems, vendors and data cross borders; and soft-law guidance dismissed as optional rather than indicative of regulator expectations.*

Where Regulation Stands Today

The regulatory posture moved materially across 2026, and boards must anticipate further shifts. The table below reflects active regulatory tracking and law firm updates as of October 2026.

Jurisdiction	Position	Source
Ghana	Cabinet approved the National AI Strategy in February 2026, followed by its official launch in April 2026. It recommends establishing an independent Responsible AI Authority. An Emerging Technologies Bill is currently under stakeholder review.	Citi Newsroom Apolitical Ministry of Communications Ghana
African Union	The Continental AI Strategy was endorsed in August 2024 as non-binding guidance. A model AI law and continental guidelines are currently being drafted for ministerial review, following consultations held in late September 2026.	Primebusiness Innovation Village
European Union	The Digital Omnibus on AI (Regulation (EU) 2026/1744) entered into force on 27 July 2026. It extends high-risk compliance deadlines for stand-alone Annex III systems to 2 December 2027, and for AI embedded in regulated products (Annex I) to 2 August 2028. Article 50 transparency obligations apply from 2 August 2026, with a transition to 2 December 2026 for the marking of AI-generated content by generative systems already on the market.	Official Journal of the EU (EUR-Lex) Gibson Dunn Sidley Austin

Jurisdiction	Position	Source
United States	No comprehensive federal statute exists. Executive Order 14365 (December 2025) directed agencies to challenge state AI laws, and a March 2026 National Policy Framework asked Congress to preempt them, but no preemption statute has passed. At state level, California's SB 53 and Texas's TRAIGA took effect on 1 January 2026. Colorado enacted SB 26-189 on 14 May 2026, replacing its 2024 law with a narrower notice and disclosure framework.	AI Wiki Blockchain Council McDermott Will & Schulte JD Supra
China	Operates without a single national AI statute. Generative AI is governed by the 2023 Interim Measures and 2025 synthetic content labelling rules. Amended Cybersecurity Law provisions took effect on 1 January 2026, and comprehensive AI legislation is listed on the State Council's 2026 agenda.	CASRAI BABL AI MLex

The takeaway for directors: Statutes shift continuously. Colorado overhauled its landmark law before enforcement began, the EU deferred high-risk deadlines by over a year, and the African Union is mid-draft on its model law. Directors cannot build oversight around moving targets. Anchor your governance in enduring fundamentals (policy, standards, inventory and risk assessments) and treat your legal obligations register as a dynamic document.

Frame: Build the Structure

Frame gives the organisation a management system to operate in and a clear view of what it is running.

The board's question: Which standard do we operate to, and can you show every AI use case we run?

- **Standards and frameworks.** The management system backbone: ISO/IEC 42001, the NIST AI Risk Management Framework, ISO 31000 and the IEEE 7000 series. Standards change more slowly than statutes, which makes them the safest foundation.
- **Inventory and intake.** A register of every AI use case, each with a named owner, including AI embedded in vendor products and staff use of public tools.

Typical gaps: *A standard adopted by name but never operated or audited, and shadow AI. A board cannot take assurance over what nobody has listed.*

Control: Manage Risk in Practice

Control turns intent into day-to-day discipline, and it is where most real incidents are either prevented or missed.

The board's question: For each use case, was a risk assessment done before go-live, what does the system itself enforce, and when was it last tested?

- **Risk classification and impact assessment.** Every use case is tiered before deployment, using approaches such as the EU AI Act risk tiers, an AI impact assessment, a data protection impact assessment and the NIST MAP function.

- **Technical guardrails.** Controls are enforced inside the system, not only described in a document. Examples include content filtering, input and output controls and access management.
- **Testing and evaluation.** Systems are tested for bias, robustness and safety, with tools and methods.

Typical gaps: *The risk assessment happens after go-live, when it can only document a decision already taken; policy text is relied on where an enforced control is needed; and a single test at launch, with no retesting when the model, the data or the use changes.*

Own: Take Accountability

Own is the theme a board holds directly, and it decides whether the other three work.

The board's question: Who is accountable, what do we see each quarter, and are the people approving high-risk use cases trained for the decision?

- **Accountability and reporting.** An AI committee, a clear RACI, model cards and regular board risk reporting that gives the board ownership and evidence.
- **People and competence.** Owners are trained and accountable. Anchors include the AI literacy provision in the EU AI Act, the competence requirement in ISO/IEC 42001, the IAPP's AIGP certification and role-based training.

Typical gaps: *Reports that count projects and pilots instead of showing risk exposure, incidents and test results, and training that reaches staff but not the directors and executives who approve high-risk use cases.*

One point runs across all four themes. Assurance means independent confirmation, not management's own account. Boards expect the three lines of defence to be visible: management owns and operates the controls, risk and compliance challenge them, and internal audit or an external reviewer tests them.

Four Questions Every Board Should Ask

A board does not need a long checklist. It needs four questions, one for each theme, and together they cover the whole subject. Use them as a standing agenda for the AI or risk committee. The right-hand column is the evidence a director should expect in reply.

Theme	Question for management	Evidence to expect
Direct	What have we committed to on AI, and what do the law and supervisors require of us in every market we touch?	Board-approved policy and risk appetite, obligations register with owners and dates, gap analysis against named guidance
Frame	Which standard do we operate to, and can you show every AI use case we run, including vendor and staff use, with a named owner?	ISO/IEC 42001 or NIST AI RMF mapping, audit results, live AI register

Theme	Question for management	Evidence to expect
Control	For each use case, was a risk assessment done before go-live, which controls does the system itself enforce, and when was it last tested?	Risk tiers and dated assessments, control inventory and access logs, test reports and retest schedule
Own	Who is accountable, what do we see each quarter, and are the people approving high-risk use cases trained for the decision?	RACI, model cards, board risk pack with incidents, training records by role

The order matters. **Direct** sets the mandate, **Frame** gives the structure and visibility, **Control** proves the risk is managed in practice, and **Own** keeps the evidence flowing to the board.

Applying This in Ghana and Across Africa

Ghana has a national AI strategy but, at the time of writing, no dedicated AI statute, so boards cannot wait for the law to tell them what to do.

The African Union has a continental framework, but not a binding law. Its Continental AI Strategy, endorsed in August 2024, sets a five-year roadmap, with national strategies and governance structures due in the first phase, 2025 to 2026. It is guidance, not regulation. The AU is now drafting guidelines and a model AI law for ministerial review, built for member states to adopt or adapt rather than apply uniformly. In the meantime, many African countries rely on their data protection laws as their main control over AI.

Four points follow for boards:

- **The stable foundations carry the weight.** Without a binding AI law, policy, standards, inventory and risk assessment are the board's main protection, alongside existing duties such as the Data Protection Act, 2012 (Act 843), which the Data Protection Commission enforces, and requirements from sector regulators such as the Bank of Ghana, the National Insurance Commission, the National Communications Authority (NCA) and the Cyber Security Authority (CSA). In healthcare, oversight is split by use case. The Food and Drugs Authority (FDA) regulates AI that works as software as a medical device or supports diagnosis, and the Health Facilities Regulatory Agency (HeFRA) licenses and inspects the facilities that deploy it. Ghana's National AI Strategy also recommends an independent Responsible AI Authority. If it is established, it would work alongside these sector bodies to set overarching safety and ethical standards.
- **Expect supervisory expectations to rise.** The national strategy recommends an independent Responsible AI Authority. Organisations that already hold an AI register and board reporting will be better placed when oversight formalises.
- **Foreign law can still reach you.** A Ghanaian firm with customers, vendors or models in the EU or elsewhere may fall within those regimes, so the obligations register under Direct must look beyond the home market. For example, the author conducted GDPR compliance assessments from Ghana for an African business with operations in Europe, demonstrating how cross-border regulatory obligations can extend beyond an organisation’s home jurisdiction.

- **Data sovereignty is a governance question.** Where data is processed, where models are hosted and who can access them are risk decisions that belong in board papers, not only in IT architecture documents.

The First 90 Days

A board can move from policy to assurance in one quarter if it sequences the work.

1. **Days 1 to 30 (Frame and Direct).** Build the AI inventory, name one accountable executive, and have the board approve an AI risk appetite statement.
2. **Days 31 to 60 (Direct, Frame and Control).** Map legal obligations across the jurisdictions you operate in, choose the operating standard, then tier every use case and complete a risk assessment for the highest tier.
3. **Days 61 to 90 (Control and Own).** Baseline test the highest-risk systems, confirm which guardrails are enforced in the systems themselves, agree the quarterly board risk pack and train directors and approvers.

AI risk will not be removed by a single policy, and it will not be contained by a single team. It is managed when each theme has an owner, a test and a line of evidence that reaches the board. Directors who can ask for that evidence, and read it critically, are the ones who will be trusted when regulators, investors and customers start asking.

Sources, Acknowledgement and Credit

The Direct, Frame, Control and Own themes make up **the Metrica360 AI Governance Model for Boards**. It builds on the AI governance themes in **Hari Kota's** "The Full AI Governance Stack". The regulatory table draws on the sources linked in it, and the primary documents, standards and tools cited are listed under References.

About the Author

Afeti Cudjoe is a strategy, technology and business transformation consultant based in Accra with more than 20 years of leadership across fintech, banking, digital transformation and ICT governance. He holds an MBA (Technology Management), an MSc (Digital Business and Innovation) and a postgraduate qualification in Cybersecurity Leadership, together with professional credentials including MCSE, CGEIT, CISA, ITIL, M_o_R, PRINCE2 and ISO. He holds an Electronics award from the City and Guilds of London, and is a member of the Engineering Council of the United Kingdom and the Institute of Internal Auditors. He has also completed global executive programmes at Harvard University in Boston, IESE Business School in New York and CEIBS Africa. Afeti advises boards through Metrica360 consulting. For more insights, follow his LinkedIn profile at linkedin.com/in/afeticudjoe.

References

Primary documents, standards and tools cited in this article. Secondary sources used for the regulation table are linked in the table.

Ghana and the African Union

1. **Ghana National AI Strategy, launch announcement.** Ministry of Communications, Digital Technology and Innovations, 24 April 2026. Ministry of Communications Ghana
2. **Data Protection Act, 2012 (Act 843).** Republic of Ghana. GhaLII
3. **Continental Artificial Intelligence Strategy.** African Union, endorsed August 2024. African Union
4. **Guideline for Registration of Software as a Medical Device.** Food and Drugs Authority (FDA), Ghana. Ghana FDA
5. **Health Institutions and Facilities Act, 2011 (Act 829).** Republic of Ghana. WHO Country Planning Cycle Database
6. **Health Facilities Regulatory Agency (HeFRA), overview.** Ministry of Health, Ghana. Ministry of Health

European Union

7. **Regulation (EU) 2024/1689 (EU AI Act).** Official Journal of the European Union. EUR-Lex
8. **Regulation (EU) 2026/1744 (Digital Omnibus on AI).** Official Journal of the European Union, published 24 July 2026. EUR-Lex

United States

9. **Executive Order 14365, Ensuring a National Policy Framework for Artificial Intelligence.** Signed 11 December 2025; Federal Register, volume 90, issue 239, 16 December 2025. Federal Register
10. **National Policy Framework for Artificial Intelligence.** White House, 20 March 2026; summary by Holland & Knight, 27 March 2026. Holland & Knight
11. **California SB 53, Transparency in Frontier Artificial Intelligence Act.** California Legislature. California Legislative Information
12. **Texas HB 149, Texas Responsible Artificial Intelligence Governance Act (TRAIGA).** Texas Legislature, signed 22 June 2025, effective 1 January 2026. Texas Legislature Online
13. **Colorado SB 26-189, Automated Decision-Making Technology.** Colorado General Assembly, introduced 1 May 2026, signed 14 May 2026. Colorado General Assembly

China

14. **Interim Measures for the Management of Generative Artificial Intelligence Services (2023).** Cyberspace Administration of China and other agencies; English translation. ANU repository

15. **Measures for Labeling of AI-Generated Synthetic Content (2025).** Promulgated 7 March 2025, effective 1 September 2025; English translation. China Law Translate

16. **Amended Cybersecurity Law of the People's Republic of China.** Effective 1 January 2026; summary by Greenberg Traurig, 12 February 2026. Greenberg Traurig

Global principles and conventions

17. **OECD AI Principles.** Adopted 2019, updated 2024. OECD.AI

18. **Recommendation on the Ethics of Artificial Intelligence.** UNESCO, 2021. UNESCO

19. **Hiroshima Process International Code of Conduct for Advanced AI Systems.** G7, published 30 October 2023. European Commission

20. **Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.** Council of Europe, opened for signature 5 September 2024. Council of Europe

Standards and frameworks

21. **ISO/IEC 42001:2023, Artificial intelligence management system.** International Organization for Standardization. ISO

22. **ISO/IEC 23894:2023, Artificial intelligence, guidance on risk management.** International Organization for Standardization. ISO

23. **AI Risk Management Framework (AI RMF 1.0).** NIST, including the Govern, Map, Measure and Manage functions. NIST

24. **ISO 31000:2018, Risk management guidelines.** International Organization for Standardization. ISO

25. **IEEE 7000-2021, Model process for addressing ethical concerns during system design.** IEEE Standards Association. IEEE SA

26. **The IIA's Three Lines Model (2020).** Institute of Internal Auditors. The IIA

Tools and certification

27. **AI Verify Foundation.** AI governance testing framework and toolkit. AI Verify Foundation

28. **Fairlearn.** Open-source toolkit for assessing and improving fairness in AI systems. Fairlearn

29. **AI Fairness 360 (AIF360).** Open-source toolkit for detecting and mitigating bias in machine learning models. GitHub

30. **promptfoo.** AI security and testing platform. Promptfoo

31. **garak.** NVIDIA's LLM vulnerability scanner. GitHub

32. **Guardrails AI.** Guardrails framework and reliability platform for AI applications. Guardrails AI

33. **NeMo Guardrails.** NVIDIA's open-source toolkit for programmable guardrails. GitHub

34. **Azure AI Content Safety.** Microsoft Azure content safety service. Microsoft Azure

35. **Artificial Intelligence Governance Professional (AIGP).** IAPP certification. IAPP

Acknowledgement

16. **The Full AI Governance Stack.** Hari Kota, infographic.

Metrica360 · info@metrica360group.com · www.metrica360group.com · Accra