



POLICY BRIEF

Evaluating Data Governance Risks Amidst AI Adoption In Nigeria

Authors: Adeniran Adedeji; Abdulkhalid Salihu;
Princess Ewa; Ebube Agbo

Four key messages



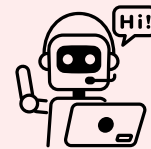
There is a strong shift toward AI adoption among digitally enabled firms, with **74%** reporting moderate to high levels of AI usage.



Costs remain the leading barrier to AI adoption, outweighing data governance concerns, with firms citing implementation and ongoing maintenance as the main challenges.



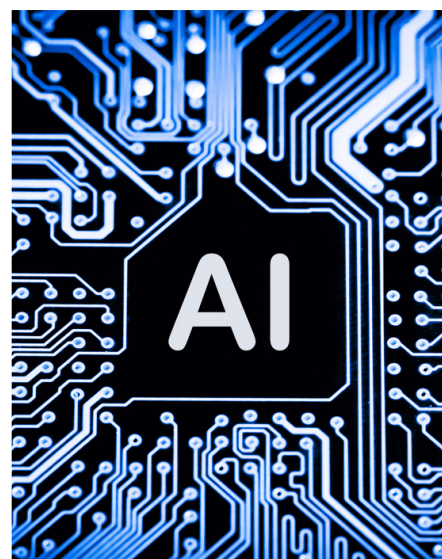
The survey highlights data privacy, cybersecurity, and the accuracy and reliability of AI systems as the key data governance concerns for firms.



Firms' responses to AI risks are largely confined to basic internal measures, such as staff training and access controls, while external mechanisms, such as independent audits or ethical boards, are less commonly identified as viable response options.

Introduction

Artificial intelligence (AI) has emerged as one of the most transformative technologies of the 21st century, with the potential to unlock trillions of dollars in economic value globally. According to PricewaterhouseCoopers (PwC), AI could contribute up to USD 15.7 trillion to the global economy by 2030, with USD 6.6 trillion coming from productivity improvements and USD 9.11 trillion from increased consumer demand.^[1] While the surge in AI adoption is most visible in advanced economies, the ripple effects are reaching emerging markets, where AI offers both opportunities and significant challenges.



For countries like Nigeria, which is in the midst of digital transformation, the question is no longer whether to adopt AI, but how to do so in a way that delivers broad-based growth while managing its emerging risks. Over the past few years, Nigeria has seen a steady rise in digital adoption. As of January 2025, about 141 million internet subscriptions were recorded, alongside a broadband penetration rate of 48.7 percent.^[2] At the same time, a growing number of firms are integrating artificial intelligence into their operations. The CSEA Survey (2025) of digitally-enabled firms reported that 74 percent have adopted AI in at least one aspect of their operations.^[3] This trend has significant implications for the country's digital economy, with the National Information Technology Development Agency (NITDA) projecting that the domestic AI market could reach USD 434 million by 2026, growing at a compound annual rate of 44.2 per cent.^[4]

While AI presents immense potential for Nigeria's growth, its transformative power is inseparable from the risks it introduces, many of which are rooted in how data is handled. Nigeria ranks 55th globally and third in Sub-Saharan Africa for data breaches, with about 10 out of every 100 citizens affected at some point.^[5] In the first half of 2025 alone, the country recorded more than 150,000 compromised accounts.^{[6][7]} This widespread vulnerability highlights vulnerability in digital infrastructure, which AI adoption could further amplify.

This brief focuses on how Nigerian firms view these emerging risks and the data governance gaps around them. It draws on new firm-level evidence to show where protections are weak and to highlight successful strategies. The aim is to guide policies that balance innovation with strong data protection and public trust.

^[1] <https://www.pwc.com/gx/en/issues/artificial-intelligence/publications/artificial-intelligence-study.html>

^[2] <https://ncc.gov.ng/market-data-reports/industry-statistics>

^[3] <https://cseaafrica.org/postdetails/artificial-intelligence-usage-in-nigeria-evidence-from-digitally-enabled-firms>

^[4] https://ncair.nitda.gov.ng/wp-content/uploads/2024/08/National-AI-Strategy_01082024-copy.pdf

^[5] <https://surfshark.com/research/data-breach-monitoring?country=ng>

^[6] <https://nairametrics.com/2025/08/01/data-breach-over-150000-nigerian-accounts-compromised-in-half-year-2025-report/>

^[7] <https://surfshark.com/research/data-breach-monitoring?country=ng>

Methodology and Data Collection

This policy brief draws on insights from the [Artificial Intelligence Usage in Nigeria: Evidence from Digitally Enabled Firms](https://cseaafrica.org/postdetails/artificial-intelligence-usage-in-nigeria-evidence-from-digitally-enabled-firms)^[8] report to examine the intersection of artificial intelligence and data governance within Nigeria's evolving digital economy. This study employed a firm-level enterprise survey to capture primary data on artificial intelligence adoption and related data governance practices in Nigeria. A total of 528 digitally enabled firms were surveyed across Lagos, Port Harcourt, and Abuja, locations chosen for their economic significance and concentration of technology-driven enterprises. The survey covered agriculture, industry, and services sectors, with firms ranging from micro to large enterprises, classified using Small and Medium Enterprises Development Agency of Nigeria (SMEDAN) standards. A structured questionnaire was administered through SurveyCTO by trained enumerators, allowing real-time monitoring and data validation. This approach ensured robust evidence from firms most likely to engage with AI, offering credible insights into the opportunities, risks, and governance gaps shaping adoption in Nigeria's private sector.

Firm Type	Number of Firms	Percentage (%)
Large Enterprise	107	20.3%
Medium Enterprise	114	21.6%
Small Enterprise	217	41.1%
Micro Enterprise	90	17.0%
Total	528	100%

^[8] <https://cseaafrica.org/postdetails/artificial-intelligence-usage-in-nigeria-evidence-from-digitally-enabled-firms>

Key Findings

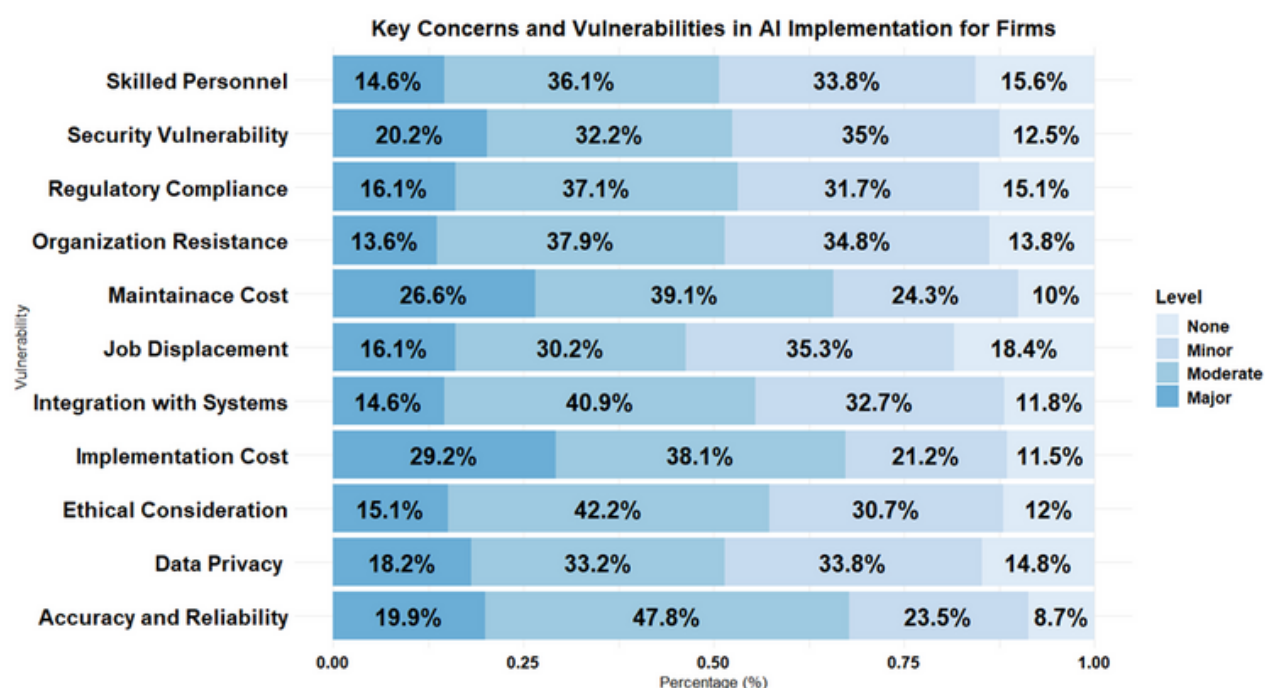
► *Concerns and Vulnerabilities of AI Adoption*



The overall evidence suggests firms do not regard data governance and ethical issues arising from AI as a major concern. Firms view most of the risks as either moderate or minor. However, some key areas were notably expressed as a major concern by a sizable number of firms. As shown in Figure 1, responses from the survey revealed that cost-related concerns weigh heavily on businesses. Implementation costs stood out, with 29% of firms surveyed identifying it as a major concern and 38.1% reporting it as a moderate concern. This aligns with the reality that many Nigerian businesses, especially SMEs, lack the financial capacity to invest in sophisticated AI tools or infrastructure. Also, 26.6% of firms cited maintenance cost as a major concern, and 39.1% as a moderate concern. In a business climate where revenue can be unpredictable and margins are tight, recurring expenses that are tied to software updates, technical support, and system upkeep can quickly become unsustainable. These concerns are consistent across firm sizes, highlighting implementation costs as a major barrier in AI adoption.

Firms also expressed concerns around accuracy, privacy, and security. While 19.9% of the respondent firms identified accuracy and reliability as a major issue, 47.8% of them saw it as a moderate concern. Similarly, while 18.2% of the surveyed firms ranked data privacy as a major concern, 33.2% of the firms reported data privacy issues as a rather moderate concern. This response reflects a growing unease around how customer or internal data is stored and used. Similarly, security vulnerabilities were reported as a major concern by 20.2% of respondents, indicating that fears around cyberattacks, system breaches, and digital sabotage are on the rise. For businesses already operating in a high-risk economic environment, these vulnerabilities feel like an additional layer of exposure they are not prepared for.

Figure 1: Concerns and Vulnerabilities of AI Adoption



Source: CSEA Survey on State of AI, 2024

Other concerns revolved around people, systems, and culture. While 14.6% of respondents flagged the shortage of skilled personnel as a major concern, 36.1% of them reported it as moderate. At the same time, integration with existing systems remains a pain point, with 14.6% citing it as a major concern and 40.9% marking it as moderate. Many firms operate with legacy systems or manual processes that do not align well with modern AI platforms, which could make integration both costly and technically challenging. On the cultural side, organisational resistance (13.6% major concern; 37.9% moderate) and ethical considerations (15.1% major; 42.2% moderate) were lower on the list but still relevant.^[9]

Moreover, concerns about job displacement were flagged by most firms as not being a significant issue, as only 16.1% of the firms surveyed considered it a major issue. This reflects a concern, as society weighs the benefits of automation against its social and human impact.

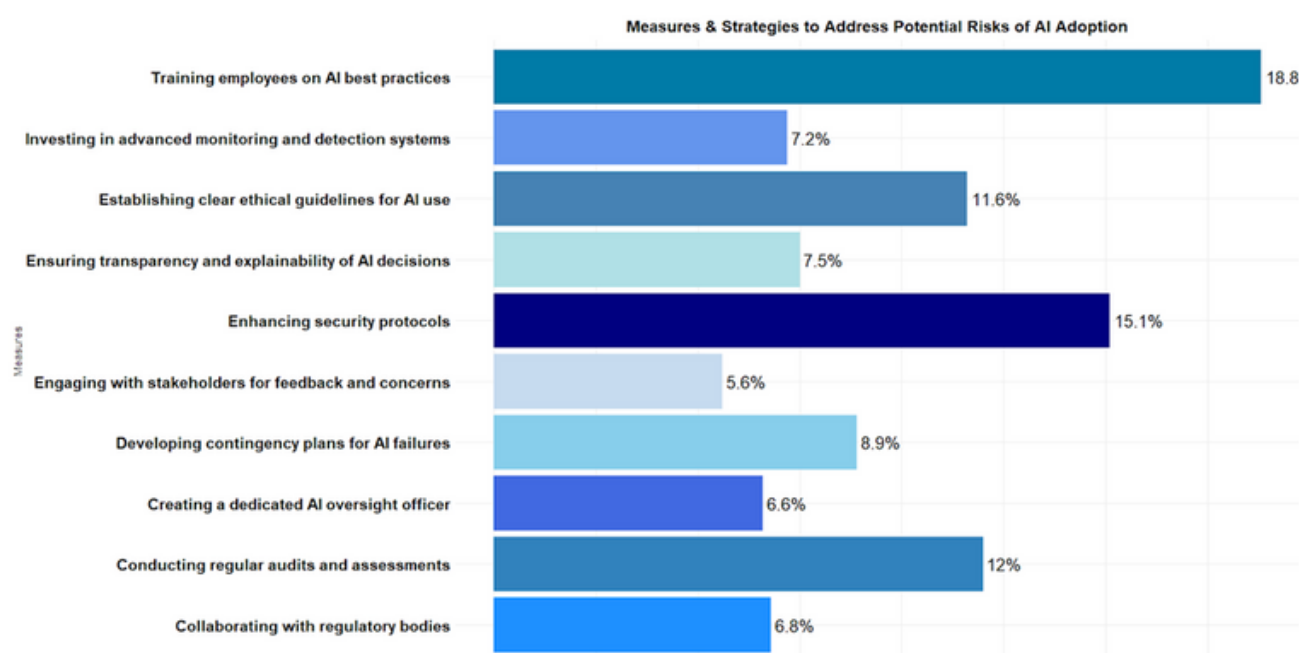
Measures to Address Concerns, Vulnerabilities, and Risks of AI Adoption

Firms are responding to the threats with different strategies. As shown in Figure 2, the survey reveals that employee training stands out as the most common strategy firms use to manage the risks of AI, with 18.8% of respondents indicating they adopt this approach. Additionally, 15.1% of firms employ enhanced security protocols, reflecting a growing concern around data breaches and cyber threats which are becoming more frequent as more businesses digitise their operations.

^[9] <https://africanmediaagency.com/africas-ai-skills-landscape-revealed-in-new-sap-report/>

Other adopted mitigation strategies include conducting regular audits and assessments (12%) and establishing ethical guidelines on AI use (11.6%). Developing contingency plans (8.9%) highlights that some firms are making preparations for possible failures or technical issues down the line. This was followed by efforts to improve transparency and explainability (7.5%) as well as investments in monitoring systems (7.2%), which indicate attempts to strengthen oversight and reliability in AI use. Fewer firms reported collaborating with regulatory bodies (6.8%) or establishing a dedicated AI oversight officer (6.6%), while stakeholder engagement ranked the lowest at 5.6%. Overall, while there is a clear effort to be proactive, the spread of responses revealed that businesses are still at different stages of preparedness, with most sticking to basic, practical steps they can control in-house.

Figure 2: Measures to Address the Risks of AI Adoption



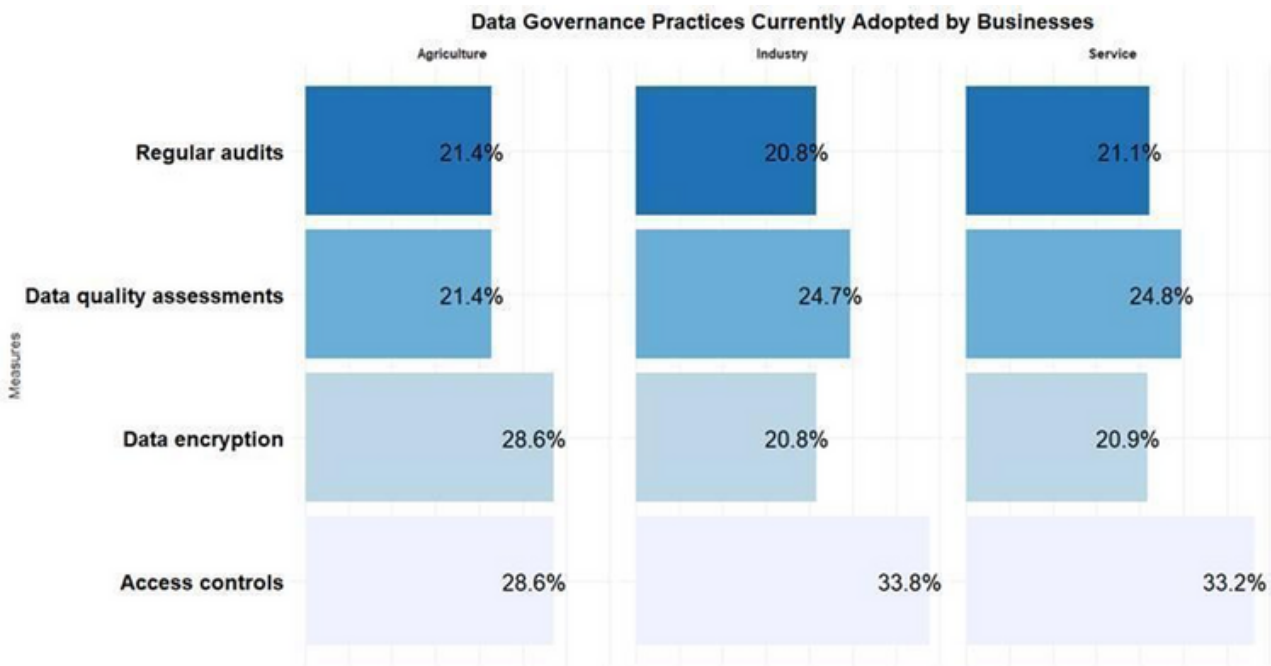
Source: CSEA Survey on State of AI, 2024

Data Governance Practices Adopted in the Face of Data Risks

The risks associated with firms' adoption of AI, such as data privacy issues, stress the need for firms to implement effective data governance practices. Data governance encompasses policies, procedures, and practices that ensure the security, quality, and usability of data.^[10] While some businesses have started implementing key data governance measures, the overall picture suggests that many are still focusing on basic protections rather than adopting a comprehensive governance approach. Patterns across different sectors reveal that businesses prioritise immediate and visible safeguards, often leaving more structured and strategic data management practices underdeveloped (see Figure 3).

^[10] <https://www.sciencedirect.com/science/article/pii/S2444569X24001379>

Figure 3: Data Governance Practices Adopted by Sector



Source: CSEA Survey on State of AI, 2024

Across the agriculture, industry, and services sectors, access control stands out as the most adopted data governance measure. In agriculture, 28.6% of firms surveyed reported implementing access controls and data encryption, while only 21.4% engaged in regular audits or data quality assessments. A similar trend is observed in the industrial sector, where 33.8% of firms reported adopting access controls, surpassing practices such as audits and encryption that were each adopted by about 20–25% of firms. The services sector, representing a significant portion of Nigeria’s economy, had the second-highest response for access control (33.2%).

The consistent preference for access control across all sectors demonstrates a practical response to immediate risks. In an environment where cyberthreats, fraud, and data breaches are increasingly common, many Nigerian firms prioritise measures that can quickly limit exposure to external threats. As digital transformation deepens, especially under growing regulatory and competitive pressures, firms will need to expand their data governance efforts beyond access controls to ensure their data remains a true asset rather than a potential liability.

Figure 4: Data Governance Practices Adopted by Firm Size



Source: CSEA Survey on State of AI, 2024

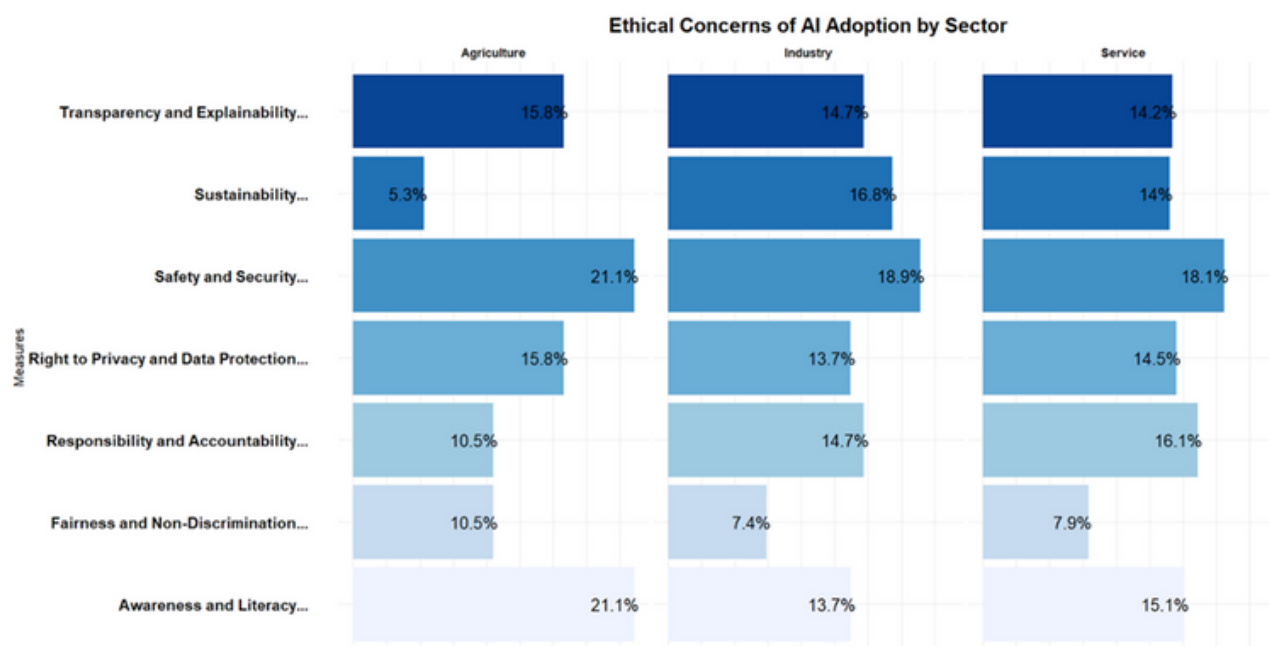
When viewed by firm size, the preference for access control remains consistent, emerging as the most widely adopted data governance practice across all categories. It accounts for over 30% of responses from large (31.7%), medium (33.1%), and small enterprises (32.4%), and rises even higher among micro enterprises at 38.1%. This implies a shared concern around external data breaches and the need to restrict unauthorised access, particularly critical for firms operating in volatile or low-trust environments. Other practices, such as data encryption, audits, and data quality assessments, are present but remain secondary, typically ranging from 20% to 25% across firm sizes (as shown in Figure 4).

Ethical Concerns About AI Adoption

AI comes with many ethical concerns, such as those around data privacy and transparency, and accountability and responsible use. These concerns have given rise to needs for ethical and responsible AI development and adoption. For firms, AI can generate economic value as well as social costs from unethical adoption. The survey also examines how firms in Nigeria are responding to the ethical considerations surrounding AI adoption.

Overall, safety and security emerged as the major ethical concern across key sectors. In agriculture, 21.1% of surveyed firms reported safety and security issues, as well as awareness and literacy, as major ethical concerns on AI adoption. Transparency, right to privacy, and fairness had slightly lower percentages. Similarly, in the industrial sector, safety and security (18.9%) is the most ethical concern, with sustainability (16.8%) also ranking relatively high. In the services sector, safety and security again led at 18.1%, followed by responsibility and accountability (16.1%) and concerns around the rights to privacy (14.5%) (see Figure 5).

Figure 5: Ethical Concerns About AI Adoption

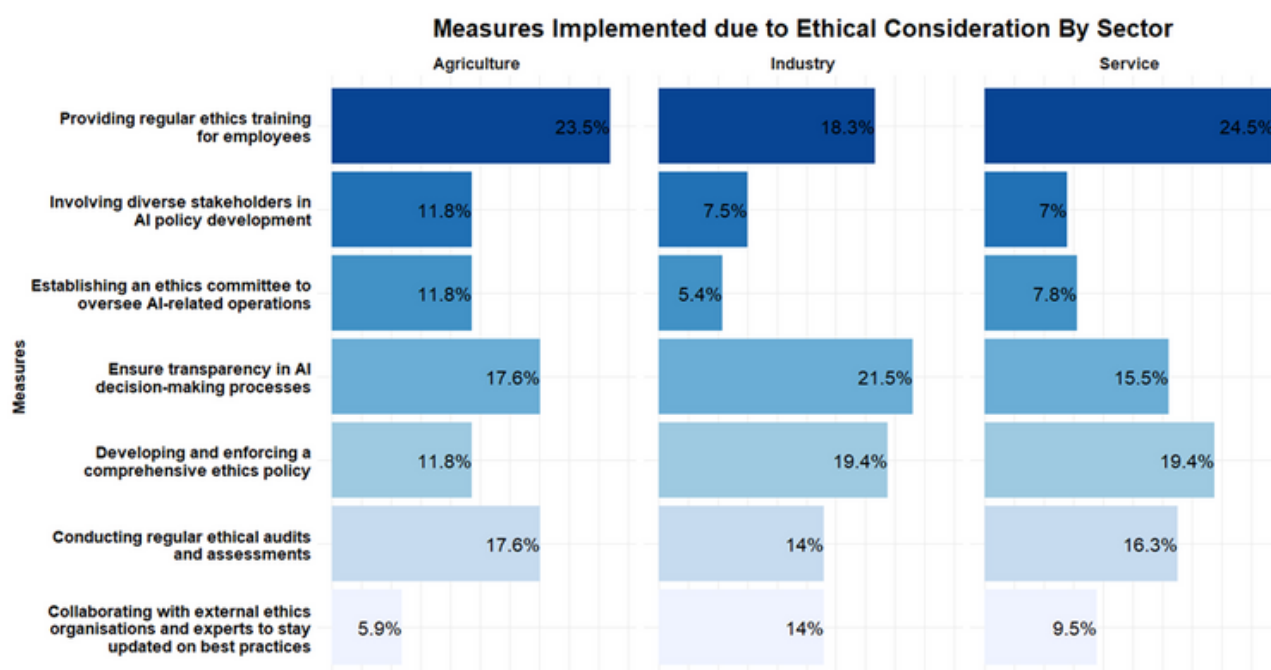


Source: CSEA Survey on State of AI, 2024

► Measures Implemented due to Ethical Considerations

While there is clear recognition of the importance of ethics in AI adoption, the level of implementation differs significantly across sectors and firm sizes. In the agricultural sector, providing regular ethics training for employees was the most commonly reported measure, adopted by approximately 23.5% of the surveyed firms. Other measures, such as conducting ethical audits or ensuring transparency in AI decision-making, were implemented by 17.6% of the firms surveyed. In the industrial sector, ensuring transparency in AI decision-making (21.5%) and enforcing comprehensive ethics policies (19.4%) were the most widely adopted practices. The relatively high attention to transparency, however, signals the sector's need to maintain credibility with clients, regulators, and international partners, especially in export-driven or highly mechanised industries. However, measures that require deeper organisational restructuring, like establishing ethics committees (5.4%) or involving diverse stakeholders in policy development (7.5%), were less frequently selected.

Figure 6: Measures Adopted due to Ethical Considerations



Source: CSEA Survey on State of AI, 2024

For the services sector, providing regular ethics training (24.5%) and developing comprehensive policies (19.4%) were the top priorities. Conducting ethical audits (16.3%) and ensuring transparency in AI decision-making (15.5%) were also relatively common. These patterns suggest that firms in the services sector operate in highly competitive environments where ethical breaches can quickly erode customer loyalty and invite regulatory sanctions. Yet, despite this proactive stance, deeper collaborative efforts, such as working with external ethics organisations (9.5%) and stakeholder involvement (7%), were still on the lower side, perhaps due to cost considerations or a general underdevelopment of independent ethics support frameworks in Nigeria (See Figure 6).

Policy Recommendations



► ***Designing AI Policies that Balance Innovation with Strong Governance***

For Nigerian firms to harness the full benefits of AI, policies must create room for firms to cut costs and innovate while at the same time protecting citizens' data and rights. A well-balanced framework should promote efficiency and competitiveness but also guard against misuse of personal information and data breaches. Embedding safeguards such as data minimisation, explicit consent, and strong accountability mechanisms within national AI regulations will help ensure that the economic gains of AI are achieved without compromising public trust and individual rights.

► ***Strengthening Regional and Global Coordination on AI Governance***

Many of the most pressing AI risks, such as cross-border data breaches, cyberattacks, and the misuse of personal information by foreign platforms, are not contained within national boundaries. Nigeria's AI governance framework must, therefore, be aligned with regional and global initiatives to ensure coherence and effectiveness. Active participation in platforms such as the African Union's digital strategy, ECOWAS frameworks, and ongoing global dialogues on AI standards will allow Nigeria to shape the rules that govern data use and protection beyond its borders. Coordinated approaches will also strengthen the country's ability to respond to cross-border threats while ensuring that local firms remain competitive in global markets.

► ***Deepening Public-Private Collaboration for Responsible AI***

The survey shows that while most firms manage AI risks through internal measures, very few recognise the value of external collaboration. This suggests the need for stronger partnerships between government, regulators, and industry. Joint initiatives, such as sector-specific guidelines, co-designed compliance toolkits, and shared reporting platforms, would ease the burden on firms while ensuring alignment with national data protection and AI standards. For the government, collaboration with the private sector offers access to real-time knowledge of market practices and emerging risks, helping to shape policies that are both practical and widely adopted.

► ***Expanding Public Awareness and Civil Society Engagement***

The Public's understanding of AI and data governance remains limited, especially outside major urban centres. Civil society organisations can help bridge this gap by translating technical standards into accessible languages and fostering community-level discussions on rights, privacy, and accountability. Policymakers, regulators, and the private sector should collaborate with these groups to design targeted campaigns and sector-specific toolkits that raise awareness while encouraging responsible adoption. This engagement will build public trust and ensure that AI serves society broadly, not just the interests of firms or government.

► ***Building Trust through Multi-Stakeholder Oversight Frameworks***

For data governance in the AI era to be effective, firms need credible and trusted structures they can engage with. Multi-stakeholder oversight bodies should, therefore, be designed not only as regulators but also as platforms that foster dialogue, guidance, and collaboration among government, industry, academia, and civil society. By creating clear frameworks for firms to report concerns, seek advice, and co-develop standards, these bodies can build the trust necessary for widespread compliance. Publishing regular reports on adoption trends, governance gaps, and enforcement actions would further strengthen accountability while showing firms that external oversight is transparent and supportive.