Central Bank of Kenya

Survey on Artificial Intelligence in the Banking Sector

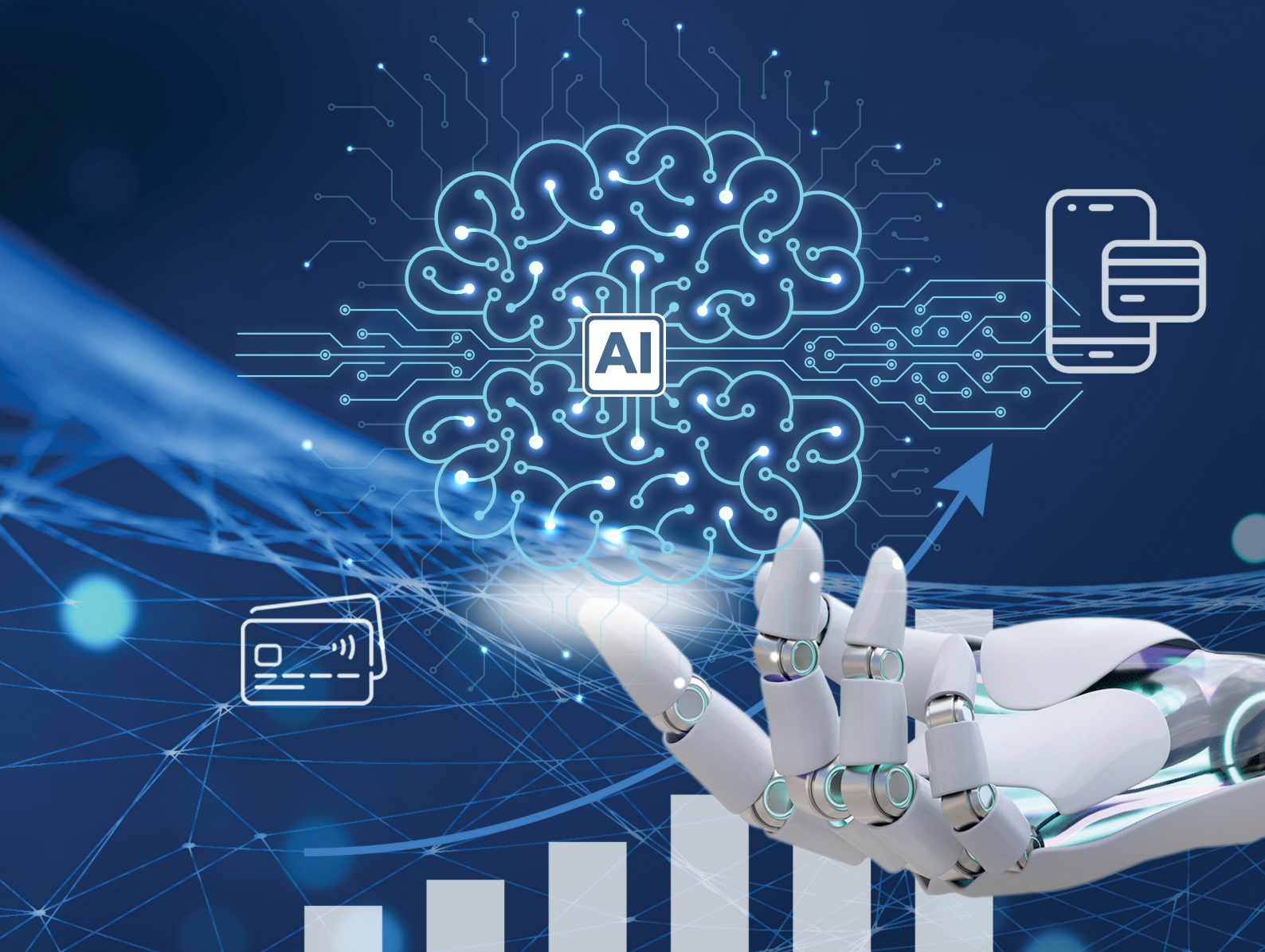

Table of Contents

List of Figures

1.0 Foreword

This report presents the results of the Survey on Artificial Intelligence (AI) in the Kenyan Banking Sector conducted in March 2025. The rise of AI is reshaping the Kenyan banking sector to streamline processes, personalize customer experiences, strengthen risk management, and drive financial inclusion.

In recognition of AI's transformative potential, the Central Bank of Kenya (CBK) has undertaken a survey to assess the current landscape of AI adoption within financial institutions, its benefits, emerging risks, and future trends. The aim of this survey is to provide valuable insights into how AI is reshaping financial service delivery, influencing consumer confidence in AI-driven solutions, and raising regulatory concerns such as ethical considerations that need to be addressed to ensure the safe and responsible use of AI.

The findings of the 2025 Survey on Artificial Intelligence in the Kenyan Banking Sector are underpinned by four broad themes:

First, the foundation of any successful AI implementation in a financial institution requires a robust strategy integrating data governance, ethical principles, and human oversight. Institutions with clearly defined AI policies and strategies have shown to be better positioned to harness AI's potential.

Second, the survey highlighted that financial institutions across the sector are actively navigating the AI maturity curve. Early adopters are embedding sophisticated AI into core functions, with the top three being credit scoring, fraud detection, and personalized customer engagement. Notably, some institutions are using Generative AI (GenAI) for operational efficiency.

Third, the survey underscored both progress and persistent challenges in AI risk management. Critical gaps remain in data quality, governance, and management. Additional risks include third-party dependencies, and limited number of skilled staff. The resource-intensiveness of AI as well as compliance challenges also continue to pose a challenge to the adoption of AI by institutions.

Lastly, the survey highlighted that there is need for regulatory guidance on AI. The proposal for CBK to issue AI guidance stems from the financial sector's need for clear governance frameworks to address emerging challenges while harnessing the benefits of AI.

CBK is committed to foster a banking environment where AI can be employed responsibly to support economic growth, safeguard consumer interests, and maintain financial stability. Accordingly, the information collected through the survey will enable CBK to provide regulatory guidance and frameworks to ensure responsible use of AI technologies.

CENTRAL BANK OF KENYA

2.0 Background

- AI systems use human and machine inputs to perceive environments, analyse them into models, and infer options for information or action. AI automates activities that require human intelligence, relying on Machine Learning (ML) and Big Data.
- In recent years, AI has been in demand in the Kenyan banking sector. The Innovation Survey 2024 Report[1] indicated that commercial and microfinance banks were likely to ramp up their innovation efforts towards developments in AI, ML, Big Data and Data Analytics in the next four years. The banking sector in Kenya is increasingly adopting AI-powered solutions to enhance efficiency and optimize decision making. This has revolutionized customer service, operations, and risk management.
- To support sustainable AI adoption, CBK conducted a survey to gather insights on AI developments and their implications for banks and policy development. The survey also aimed to assess the extent of AI adoption in financial institutions, understand the key benefits and challenges of such adoption, and identify emerging trends in the industry. Further, the survey collected insights on how the banking sector is mitigating risks that arise from the adoption of AI.

2.1 Survey Methodology

- The survey collected data on the state of innovation as of December 31, 2024, from 37 commercial banks, 1 mortgage finance institution, 14 microfinance banks (MFBs), 3 Credit Reference Bureaus (CRBs) and 70 Digital Credit Providers (DCPs).
- The survey was issued in March 2025.
- Questions in the survey were classified into 4 sections:
  - **Section A** – AI and Data Strategy.
  - **Section B** – Institution AI Activities.
  - **Section C** – AI Risk Management.
  - **Section D** – Impact and Challenges.

2.2 Executive Summary

- 50 percent of the survey respondents indicated that they had adopted AI. Notably, all CRBs indicated that they had not adopted the use of AI in their operations. However, one out of three CRBs indicated that they were experimenting the use of AI and had allocated resources to support the adoption of AI in future.
- 70 percent of respondents indicated that they did not have AI Strategies, while 30 percent had established AI Strategies.
- Out of the institutions which had adopted AI, 41 percent of the respondents had implemented AI policies while 59 percent had not.
- 51 percent of respondents indicated that they had established dedicated Data/AI teams.
- Out of the institutions that had implemented AI, 63 percent indicated that they actively monitored ethical considerations of their AI Models to prevent unintended consequences for AI use while 37 percent indicated they did not monitor these aspects.
- 68 percent of survey respondents who had adopted AI indicated that they were using generative AI Tools and frameworks in their operations.

1 https://www.centralbank.go.ke/uploads/banking_sector_reports/1736029340_Banking%20Sector%20Innovation%20Survey%202024.pdf

- 46 percent of institutions developed AI applications in-house, 40 percent outsourced the development, and 24 percent partnered with other entities for development of AI applications.
- 35 percent of respondents used third-party service providers for AI/ML services while 17 percent indicated that the partnerships included AI and FinTech start-ups.
- Based on Gartner's AI Maturity Model Levels,[2]
    - 54 percent of respondents indicated that they were at Level 1 of AI maturity (Awareness), with an early interest and few exploratory AI initiatives.
    - 13 percent of institutions were at Level 2 of AI maturity (Active), with pilots, experiments, and allocation of resources to AI.
    - 19 percent of institutions were at Level 3 of AI maturity (Operational), with some usage in workflows, and establishment of initial AI governance processes.
    - 4 percent were at Level 4 of AI maturity (Systemic), with use in workflows and operations for new business models.
    - 1 percent were at Level 5 of AI maturity (Transformational), leverage extensive use of AI to create new products, services, and business models, achieving a competitive advantage.
    - 9 percent of the respondents indicated that they had not considered using AI.
- The top three applications of AI and ML by respondents were credit risk assessment at 65 percent, cybersecurity at 54 percent, and customer service at 43 percent. This was followed by electronic Know Your Customer (e-KYC) at 41 percent and fraud risk management at 40 percent.
- 83 percent of institutions indicated that they were likely to adopt AI for credit risk assessment in future, and 82 percent for cybersecurity, customer service, and e-KYC.
- The leading risks reported by institutions that use AI include data quality, governance, and management (59 percent), cybersecurity risks (54 percent), limited numbers of AI-skilled staff (52 percent), third-party dependencies (52 percent) and AI governance risks (51 percent).
- 56 percent of the institutions that had adopted AI had put in place measures to ensure the AI models are explainable.
- 73 percent of the institutions' customers had equal access to the benefits of the AI models.
- 78 percent of institutions indicated that AI had enhanced their performance and operational efficiency.

2 **Gartner's AI Maturity Model Levels:**
Level 1: Awareness
- Organizations have an early interest in AI and are starting to have conversations around AI strategy.
- AI initiatives are mostly experimental and exploratory.

Level 2: Active
- Initial experimentation and pilot projects with AI are underway.
- Organizations begin to see the potential value of AI and start to allocate resources.

Level 3: Operational
- AI is used in at least one workflow or business process.
- Organizations have established some AI governance and management practices.

Level 4: Systemic
- AI is present in the majority of workflows and operations.
- AI initiatives inspire new digital business models and drive significant business value.

Level 5: Transformational
- AI is inherent in the DNA of the business
- Organizations leverage AI to create new products, services, and business models, achieving a competitive advantage.

Source: https://www.gartner.com/en/documents/3982174

- The top three challenges in the adoption of AI were shortage of skills (46 percent), high costs and limited resources (46 percent), and governance and regulatory compliance challenges (43 percent).

- 93 percent of institutions surveyed recommended that CBK should issue Guidance on AI covering the following areas:

  - Governance and compliance.
  - Risk management frameworks.
  - Incident management and reporting.

3.0 Survey Findings

3.1 AI and Data Strategy

3.1.1 Institutions' Adoption of AI

- 50 percent of the survey respondents indicated that they had adopted AI as illustrated in **Figure 1.** This comprised 66 percent of commercial banks, 57 percent of MFBs, and 43 percent of DCPs.
- Notably, all CRBs indicated that they had not adopted the use of AI in their operations as outlined in **Figure 2** below.

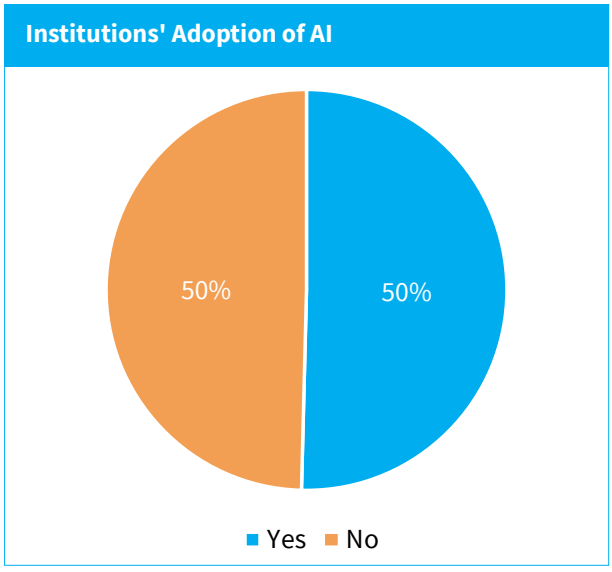

Figure 1: Institutions' Adoption of AI

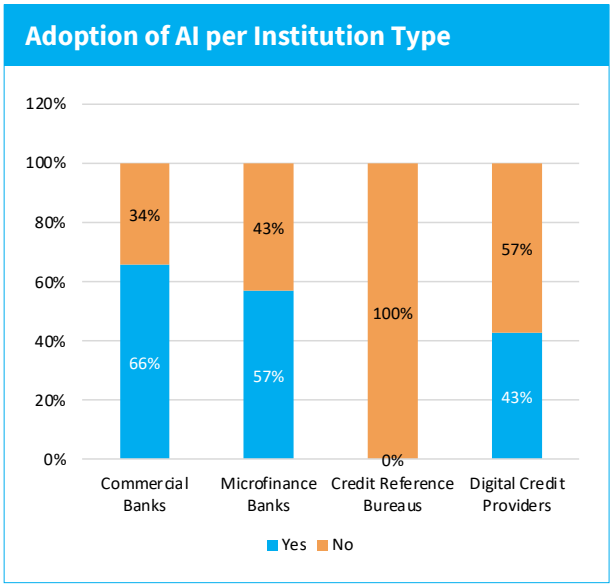

Figure 2: Adoption of AI per Institution Type

3.1.2 Adoption of AI Strategies

- 70 percent of respondents indicated that they did not have AI Strategies, while 30 percent had established AI Strategies.

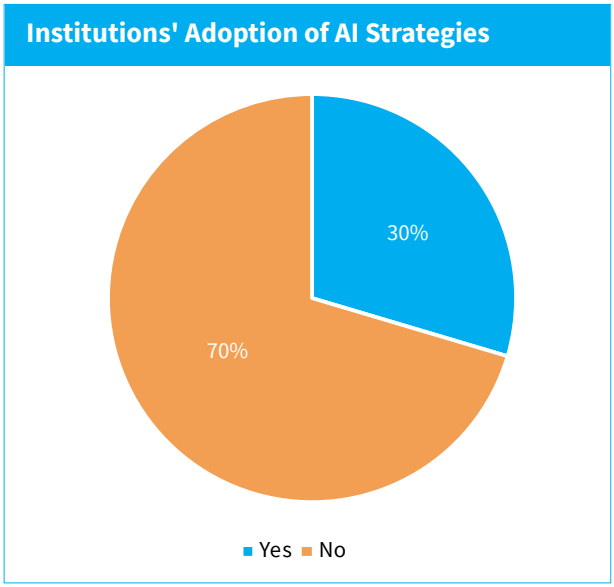

Figure 3: Institutions' Adoption of AI Strategies

- Institutions with AI strategies comprised 29 percent of commercial banks, 36 percent of MFBs, none of the CRBs, and 30 percent of DCPs.

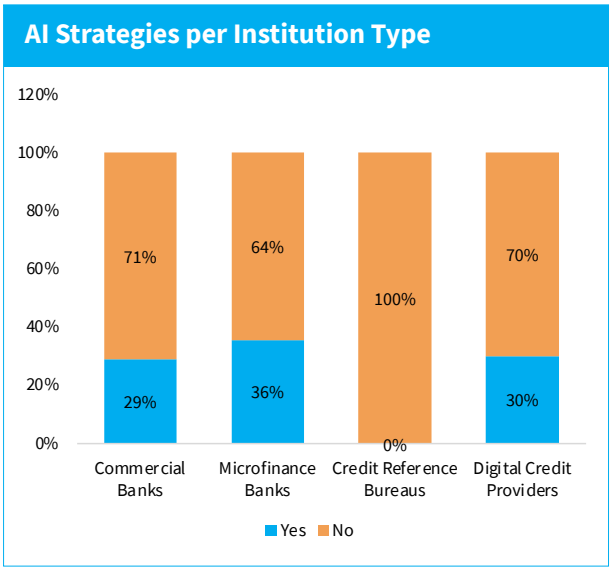

Figure 4: AI Strategies per Institution Type

- Some institutions had integrated AI into their broader data or innovation strategies. However, others demonstrated mature, well-governed AI frameworks that included ethical principles, model explainability, and regulatory alignment.
- The AI strategies employed by the surveyed institutions covered the following areas:
  - Business objectives and use cases of AI in the institution, including:
    - Credit scoring.
    - Fraud prevention and detection.
    - Transaction monitoring.
    - Customer service.
    - Data analytics.
    - Financial education.
    - Business insights.
    - Forecasting.
    - Wealth management.
    - Quality assurance.
    - Digital accessibility for persons with disability.
    - Automation of operations.
  - AI and data governance.
  - AI ethics and principles including fairness, transparency, explainability, accountability, human-centricity, and inclusion and prevention of bias.
  - Data confidentiality, validation, and processing.
  - Risk management of third-party risks, cyber risk, model risk, and privacy risk.
  - Technology stack/infrastructure required.
  - Model development and deployment.
  - Performance evaluation and continuous model improvement.
  - Change management.
  - Talent development.
  - Partnerships with ecosystem and regulators.
  - Investment and resources.
  - Legal and compliance issues.
  - Impact assessment.
  - Implementation roadmap.

3.1.3 Adoption of Data Strategies

- 62 percent of the institutions surveyed had established data strategies. This comprised 66 percent of commercial banks, 57 percent of MFBs, 100 percent of CRBs and 59 percent of DCPs.

- The proportion of institutions with data strategies is represented as per Figure 5 and **Figure 6** below.

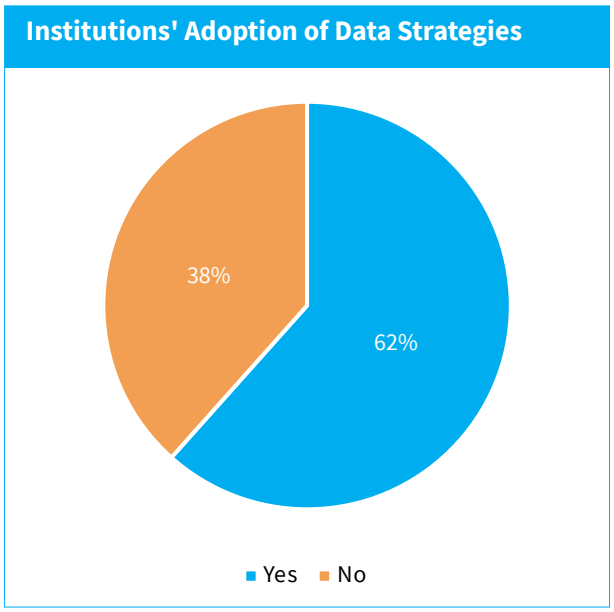

Figure 5: Institutions' Adoption of Data Strategies

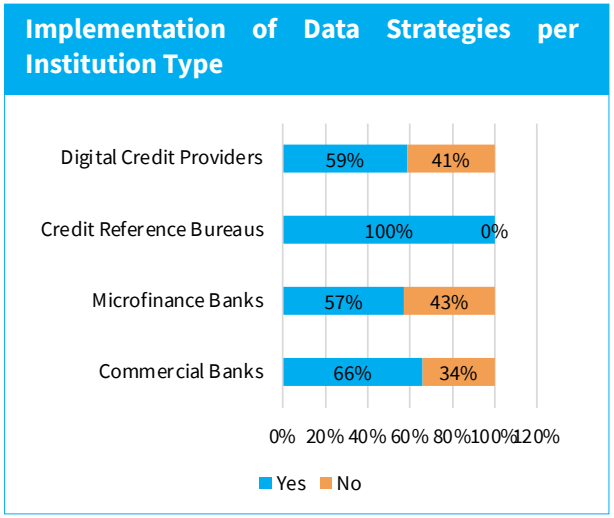

Figure 6: Implementation of Data Strategies per Institution Type

- Of the institutions that had adopted AI, 72 percent of commercial banks, 88 percent of MFBs and 80 percent of DCPs had implemented data strategies, as illustrated below.

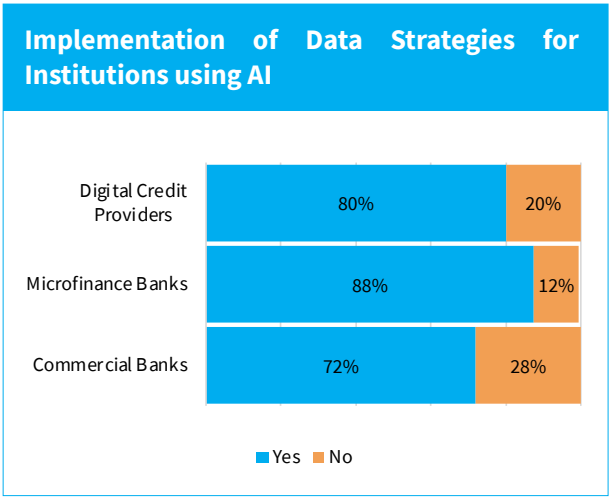

Figure 7: Implementation of Data Strategies for Institutions using AI

- The data strategies covered critical areas including:
  - Data governance.
  - Data privacy and protection.
  - Data architecture.
  - Data security.
  - Data quality.
  - Data collection.
  - Data management.
  - Data utilization.
  - Data integration into the institutions' applications.
  - Use of AI in data analysis.
  - Data storage and retention.

3.1.4 Institutions' Implementation of AI Policies

- Out of the institutions which had adopted AI, 41 percent of the respondents had implemented AI policies while 59 percent had not.
- The institutions with AI policies comprised 36 percent of commercial banks, 38 percent of MFBs, and 47 percent of DCPs.

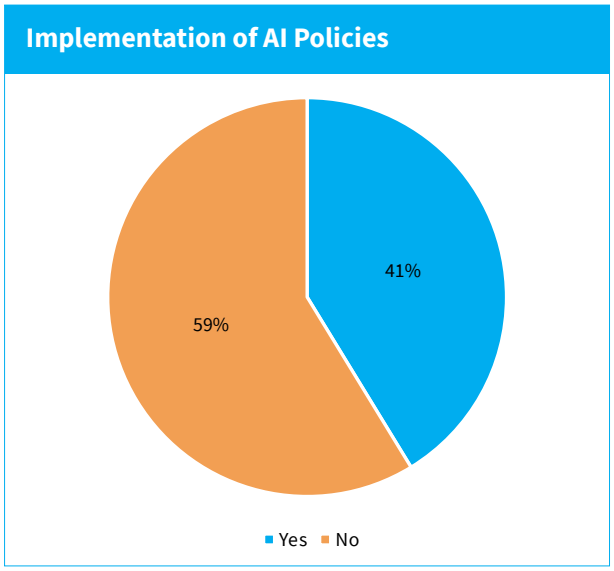

Figure 8: Implementation of AI Policies

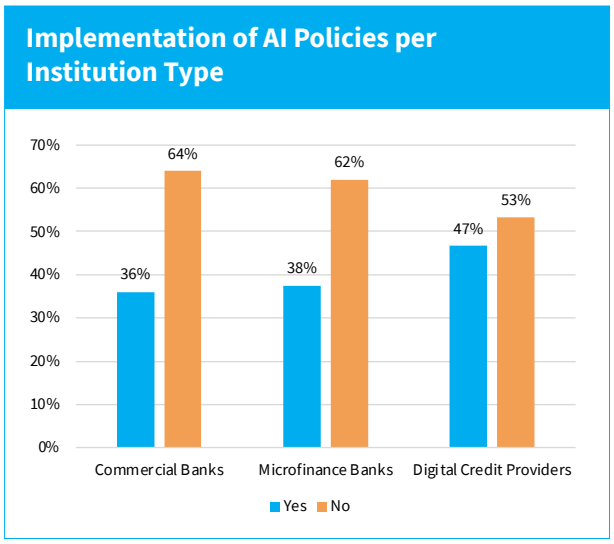

Figure 9: Implementation of AI Policies per Institution Type

- The AI policies adopted by institutions covered the following areas:
  - Approved AI use cases and alignment with business values and goals.
  - Guiding principles: fairness, bias mitigation, reliability, inclusiveness, security, accountability, interpretability, human-centricity, and transparency.
  - Governance and compliance.
  - Establishment of AI Governance Committees.
  - Ethical and responsible AI standards.
  - Roles and responsibilities of staff, vendors, and developers.
  - Ethical and responsible AI development and deployment.
  - Risk management.
  - Data quality, management, and usage.
  - Data privacy and security.
  - Training and awareness.
  - Talent planning.
  - Legal compliance.
  - Intellectual Property rights and attribution.
  - Customer engagement.
  - Monitoring and evaluation.
  - Model design.
  - Documentation.
  - Human governance and oversight of models.
  - Violations and reporting.
  - Stakeholder communication.
  - Interconnected policies/standards within the organization.

3.1.5 Dedicated Data/AI Teams and Team Composition

- 51 percent of respondents indicated that they had established dedicated Data/AI teams.

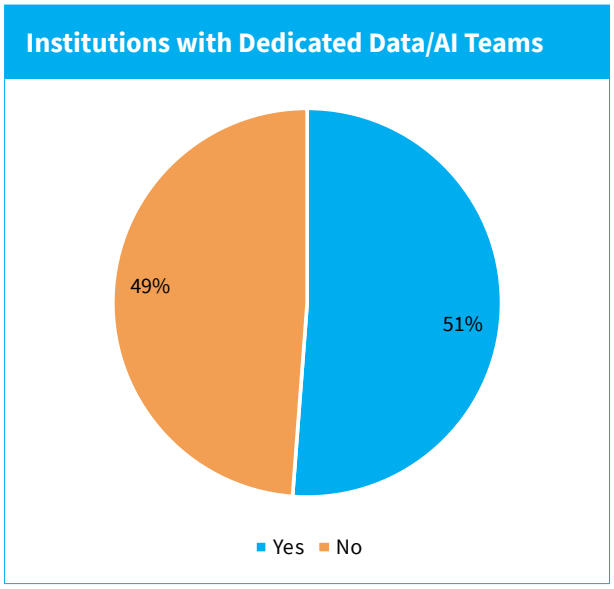

Figure 10: Institutions with Dedicated Data/AI Teams

- The dedicated Data/AI Teams by institutions are made up of data analysts. Specific team roles included:
  - Data analysts.
  - Data architects.
  - Data scientists.
  - Data engineers.
  - Machine learning/software engineers.
  - Data owners.
  - Data stewards.
  - Data champions.
  - Data management and quality assurance specialists.
  - Data governance and compliance specialists.
  - Business intelligence specialists.
  - Risk management specialists.
  - Technology managers.
  - Executive leadership.

3.1.6 Technology Platforms in Support of Data/AI Strategy

- Institutions had adopted various technology platforms to support their data and AI strategies. The top technology tools used were data visualization and business intelligence tools (68 percent), cloud computing platforms (64 percent), and collaboration and version control tools (52 percent).
- The least adopted technological tools were Machine Learning and AI Platforms at 36 percent, and development operations (DevOps)[3] and machine learning operations (MLOps)[4] at 37 percent adoption rate.

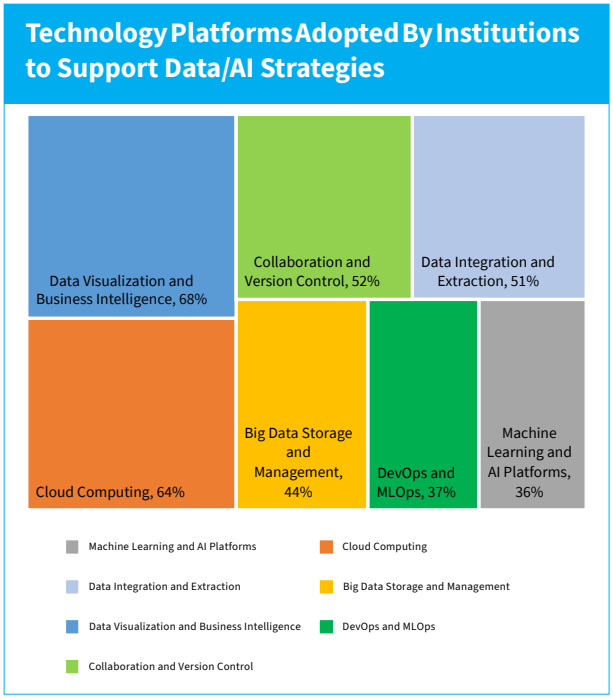

Figure 11: Technology Platforms Adopted by Institutions to Support Data/AI Strategies

3 Development Operations (DevOps) is a software development methodology that accelerates the delivery of high-performance applications and services by combining and automating the work of software development (Dev) and Information Technology (IT) operations (Ops) teams. It focuses on improving collaboration between software development and IT operations teams by streamlining workflows, enhancing automation, and accelerating the deployment of applications using tools and monitoring systems. Source: https://www.ibm.com/think/topics/devops

4 Machine Learning Operations (MLOps) extends DevOps principles to machine learning projects. It aims to automate and improve the lifecycle of ML models, including model training, deployment, monitoring, and governance. It ensures reproducibility, scalability, and reliability in ML applications. Source: https://www.ibm.com/think/topics/mlops

3.1.7 Ethical Oversight in AI Model Development

- Out of the institutions that had implemented AI, 63 percent indicated that they actively monitored ethical considerations of their AI Models to prevent unintended consequences for AI use while 37 percent indicated they did not monitor these aspects.

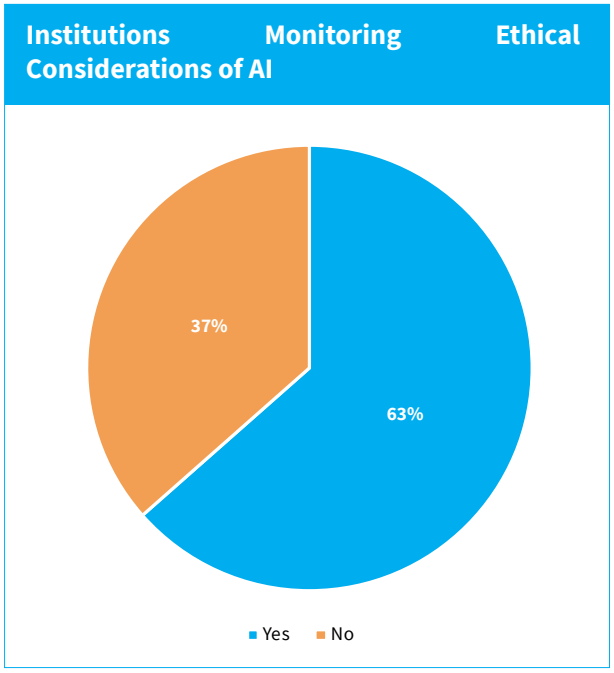

Figure 12: Institutions Monitoring Ethical Considerations of AI

- The methods used by institutions to monitor AI models for ethical considerations were:
  - Strong prioritization of data and cyber security measures.
  - Verifying that correct data is used for training AI models.
  - Data anonymization.
  - Bias detection and mitigation.
  - Use of alternative and diverse data sources for increased accuracy.
  - Manual analysis for comparison with model output.
  - Enhancing explainability and transparency.
  - Human oversight, including permitting the appeal of AI-generated decisions through a human review process.
  - Adherence to data privacy and security regulations and measures.
  - Continuous monitoring and feedback loop.
  - Stakeholder engagement, training, and awareness.
  - Audit of AI models.
  - Research programs for quantifying, monitoring, improving fairness in ML models.
  - Subjecting AI ethics to broader institution's Code of Conduct and Ethics.
  - Development and implementation ethical guidelines for AI development and deployment.
  - Documenting data sources, algorithms, and model limitations.
  - Providing clear explanations to users about AI driven decisions.
  - Defining clear lines of accountability.
  - Developing protocols for addressing AI related errors.
  - Testing models using different scenarios.
  - Establishing an AI committee to oversee AI governance in the organization.
  - Establishing AI Framework., Code of Ethics and Conduct Framework, and Model Risk Governance Framework.

3.1.8 Mechanisms Adopted by Institutions to Support AI Strategy

- The growth of artificial intelligence (AI) has brought to the fore the need for institutions to adopt various mechanisms to ensure responsible and effective implementation. For institutions, The top three mechanisms adopted by institutions to support their AI strategies as illustrated in Figure 13 below are:
  - Implementation of data governance frameworks (79 percent).
  - Access to training and human oversight (70 percent).
  - Implementation of cybersecurity measures and operational resilience for AI applications (62 percent).
- 17 percent of respondents indicated that they adopted the following other mechanisms to support their AI strategies:
  - Establishing risk governance committees.
  - Ramping up in-house expertise.
  - Strategic partnerships and collaboration with industry experts.
  - Collaboration among cross-functional teams, including IT, business units, and compliance teams.
  - Robust AI governance and ethics frameworks.
  - Automation of AI monitoring tools.
  - Pilot projects and iterative testing.

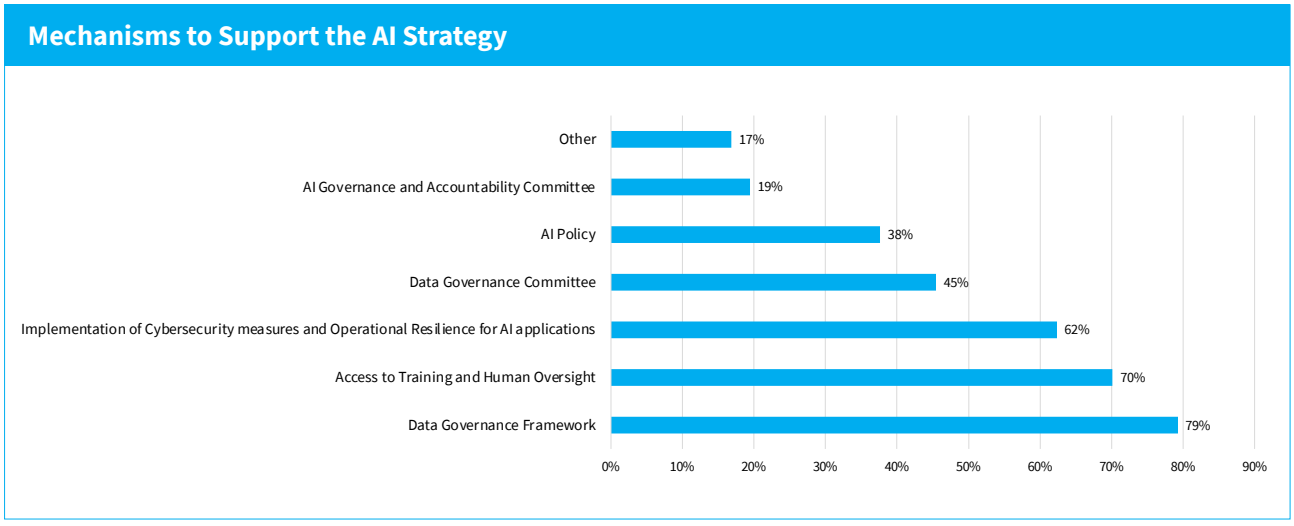

Figure 13: Mechanisms to Support the AI Strategy

3.1.9 Synthetic Data for AI Model Training

- 16 percent of respondents that had implemented AI indicated that they used synthetic data to train AI models.

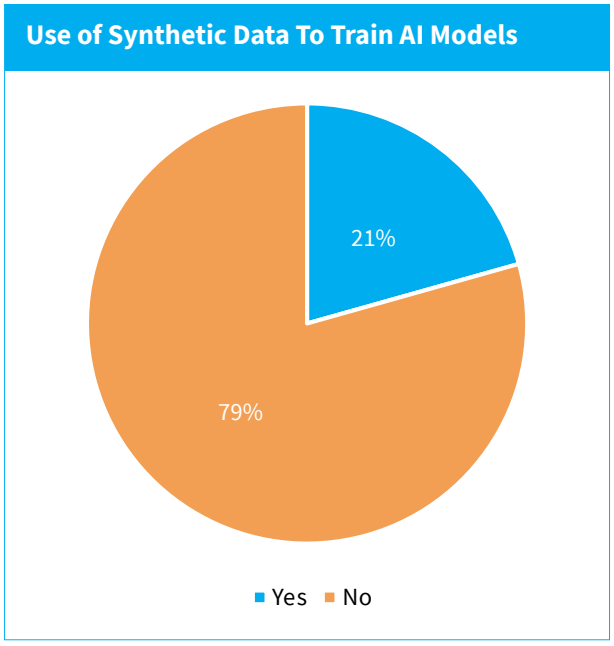

Figure 14: Use of Synthetic Data to Train AI Models

3.1.10 Utilization of Generative AI Tools and Frameworks

- 68 percent of survey respondents that had adopted the use of AI indicated that they were using generative AI Tools and frameworks in their operations.
- This comprised 68 percent of commercial banks, 63 percent of MFBs, and 70 percent of DCPs.

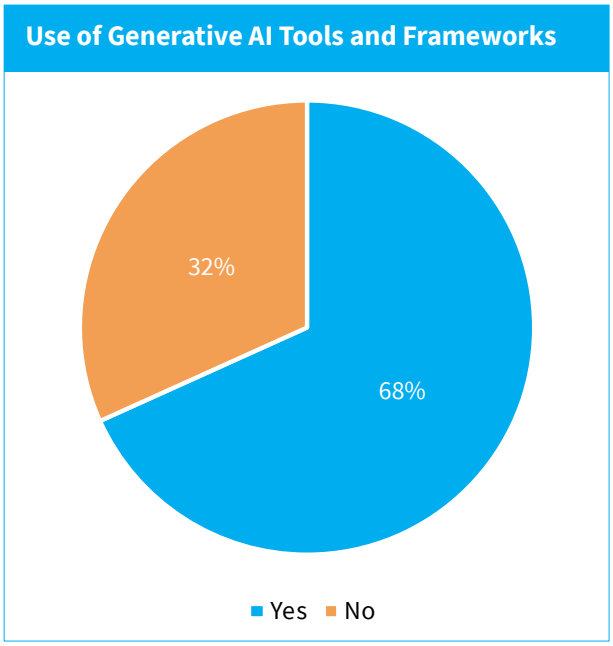

Figure 15: Use of Generative AI Tools and Frameworks

3.1.11 In-house Development, Outsourcing for AI Applications and Partnerships

- Financial institutions have adopted different approaches in the implementation and usage of AI based applications based on their operational needs, resource availability, and strategic goals.
- 46 percent of institutions that had adopted AI developed the AI applications in-house, 40 percent outsourced the development, and 24 percent partnered with other entities for development of AI applications.

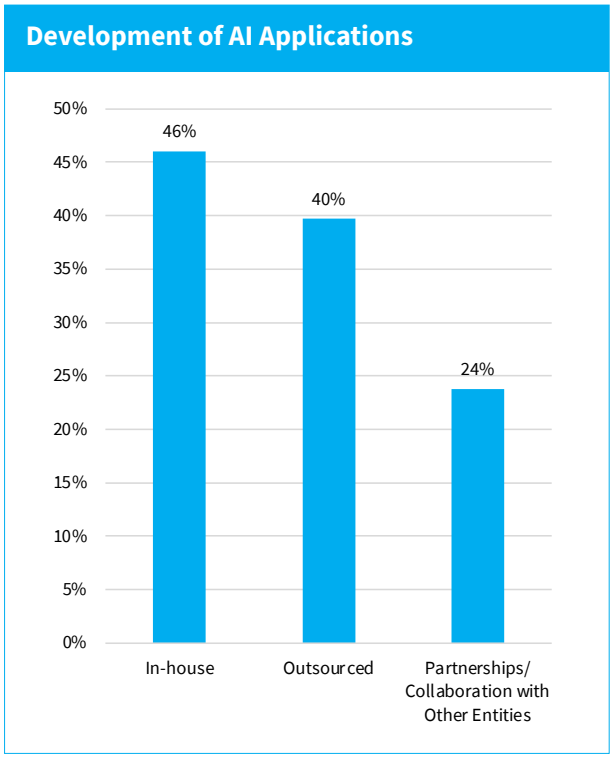

Figure 16: Development of AI Applications

3.1.12 Third-Party AI/ML Service Providers

- 35 percent of respondents that had implemented AI used third-party service providers for AI/ML services while 17 percent indicated that the partnerships included AI and FinTech start-ups.
- Institutions partnering with third-party AI services providers comprised 42 percent of commercial banks, 12 percent of MFBs, and 46 percent of DCPs.

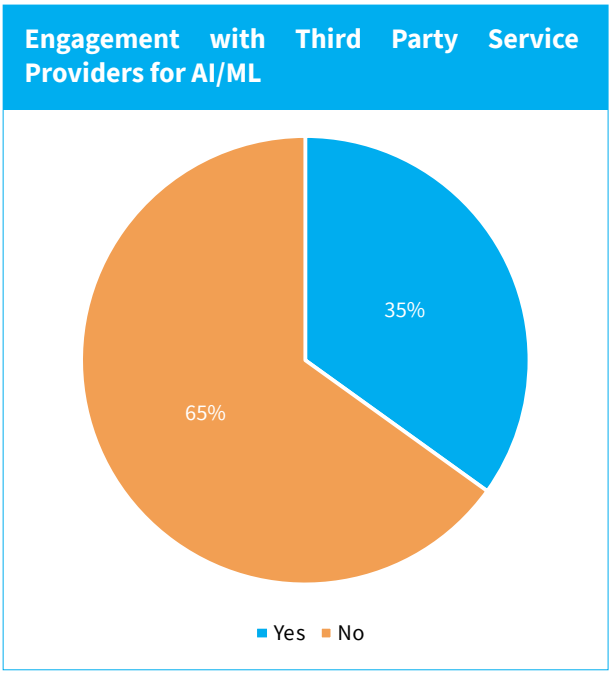

Figure 17: Engagement with Third-Party Service Providers for AI/ML

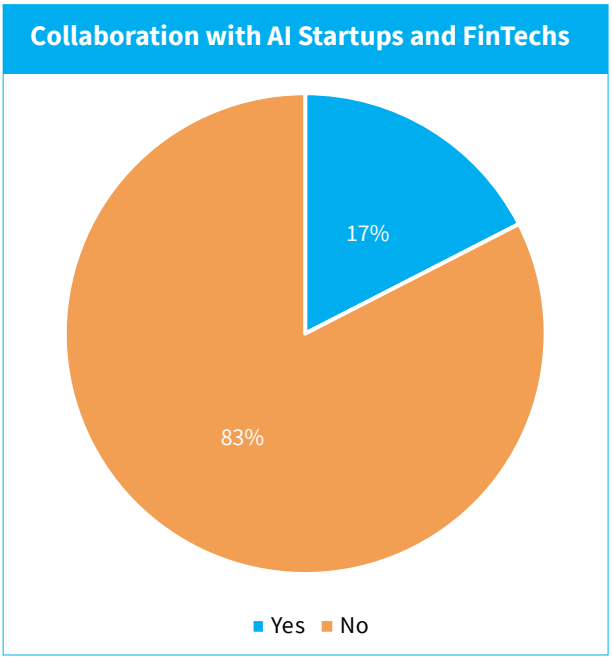

Figure 18: Collaboration with AI Startups and FinTechs

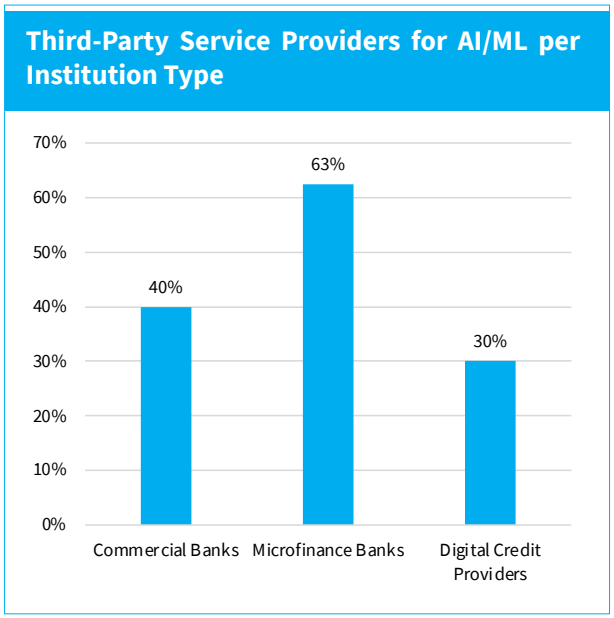

Figure 19: Third-Party Service Providers for AI/ML per Institution Type

- The services provided by third-party AI service providers included:
  - Customer credibility and credit scoring.
  - Data processing: OCR image recognition and data transformation for credit listing.
  - Threat detection and anomaly monitoring.
  - Financial crime monitoring, particularly for transaction monitoring and behavioural analysis.
  - Model development and optimization.
  - Marketing and customer engagement.
  - Productivity tools.
- Key controls that had been put in place by institutions using third-party service providers included:
  - **Data Privacy and Protection:** All data shared with third parties is anonymized and personally identifiable information is excluded. Institutions have established strong encryption, masking, and privacy safeguards. Third-party providers are bound by data privacy agreements and compliance with regulations.
  - **Cybersecurity:** Role-based access, least privilege principles, and audit trails applied for third-party AI service providers. AI-powered cybersecurity solutions further strengthened digital defences against evolving threats.
  - **Vendor Risk Management:** Institutions are pursuing vendor due diligence and conducting onboarding evaluations in vetting the third-party service providers before they are engaged, periodic audits, performance reviews, and risk assessments.
  - **Model Risk Management (MRM):** Institutions reported having independent model validation processes, testing for accuracy, fairness, bias, and interpretability, and continuous monitoring of AI model behaviour and output in ensuring data safety as they use the services of third parties.
  - **Governance and Ethical AI Use:** Governance measures encompassed contractual agreements adhering to global regulations such as the European Union's General Data Protection Regulations (GDPR), and vendor oversight through periodic reviews and risk assessments.

3.2 Institutions' AI Activities

3.2.1 Artificial Intelligence (AI) Maturity Levels

- Respondents were requested to rank themselves based on Gartner's AI Maturity Model Levels.
- 54 percent of respondents indicated that they were at Level 1 of AI maturity (Awareness), with an early interest and few exploratory AI initiatives.

- 13 percent of institutions were at Level 2 of AI maturity (Active), with pilots, experiments, and allocation of resources to AI.
- 19 percent of institutions were at Level 3 of AI maturity (Operational), with some usage in workflows, and establishment of initial AI governance processes.
- 4 percent were at Level 4 of AI maturity (Systemic), with use in workflows and operations for new business models.
- 1 percent were at Level 5 of AI maturity (Transformational), leverage extensive use of AI to create new products, services, and business models, achieving a competitive advantage.
- 9 percent of the respondents indicated that they had not considered using AI.
- A summary of the level of maturity per institution is shown in Figure 20 below.

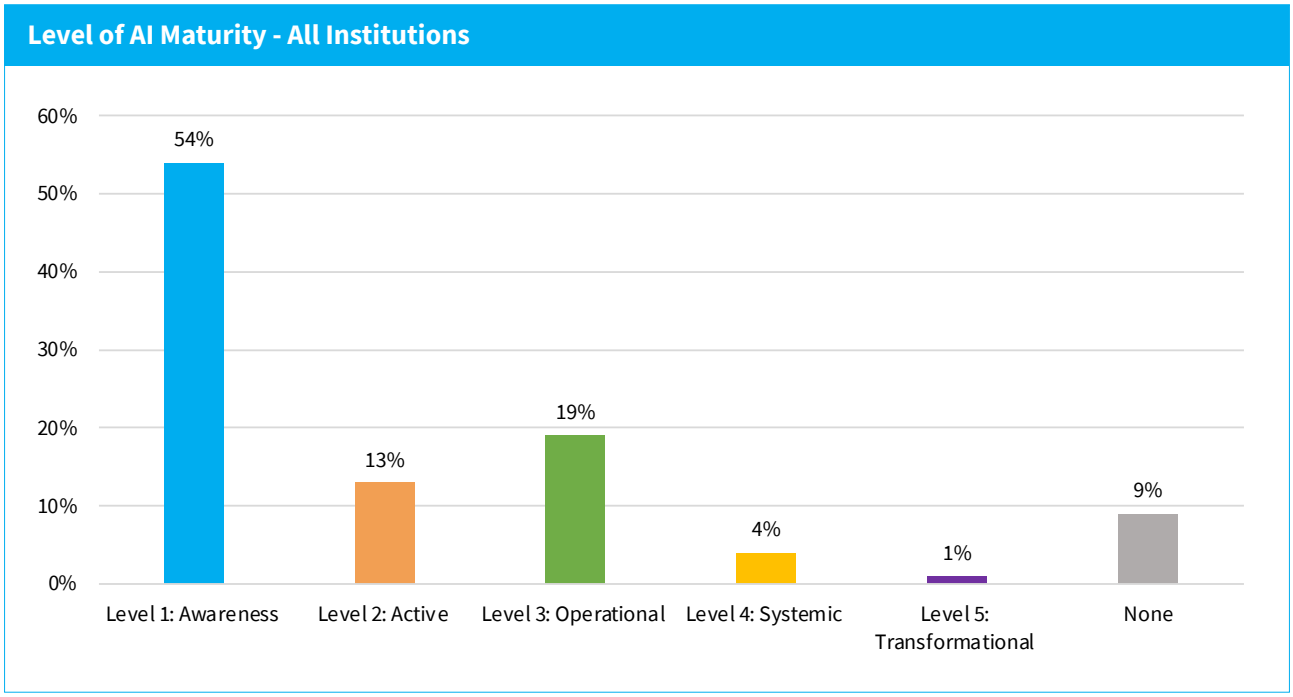

Figure 20: Level of AI Maturity - All Institutions

- Below is the level of AI maturity as a percentage aggregated by institution type and the corresponding level of maturity.

Level of AI Maturity per Institution Type

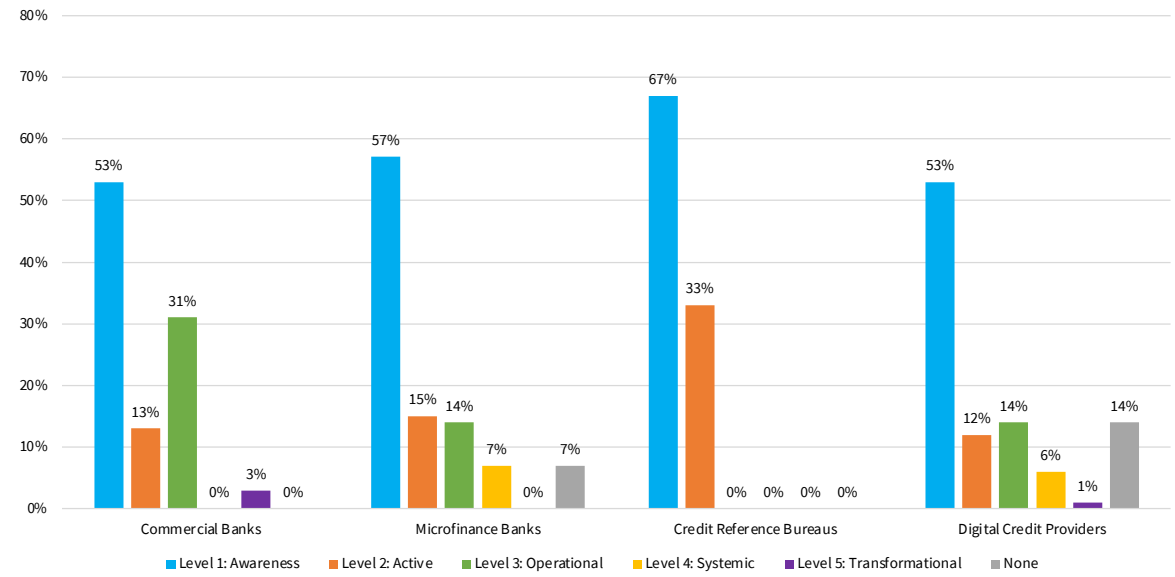

Figure 21: Level of AI Maturity per Institution Type

3.2.2 Practical Applications of AI and ML by Financial Institutions

- The top three applications of AI and ML by institutions that had adopted AI were credit risk assessment at 65 percent, cybersecurity at 54 percent, and customer service at 43 percent. This was followed by e-KYC at 41 percent and fraud risk management at 40 percent.
- AI was least used in algorithmic trading at 5 percent of respondents, personal financial management at 8 percent, and financial literacy at 11 percent.

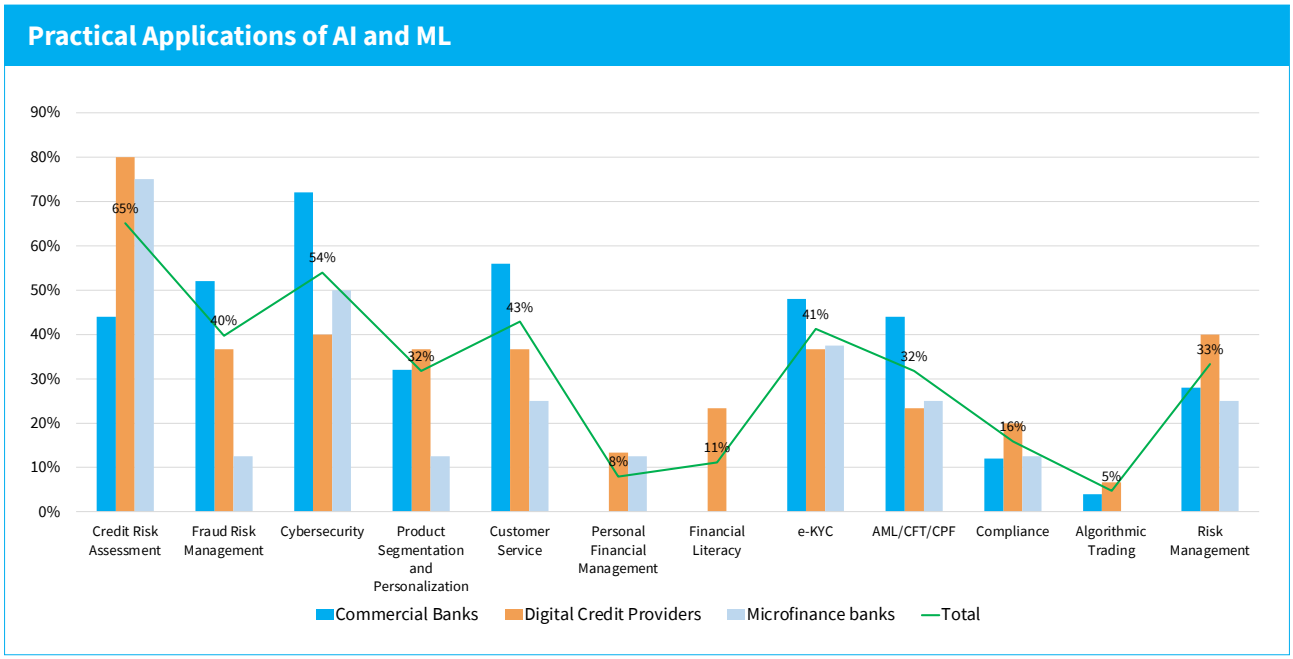

Figure 22: Practical Applications of AI and ML

- Institutions further indicated that they utilized AI in software development to enhance coding efficiency, debug errors, and generate code.
- 83 percent of institutions indicated that they were likely to adopt AI for credit risk assessment in future, followed closely by customer service, cybersecurity, and e-KYC at 82 percent each as illustrated below.

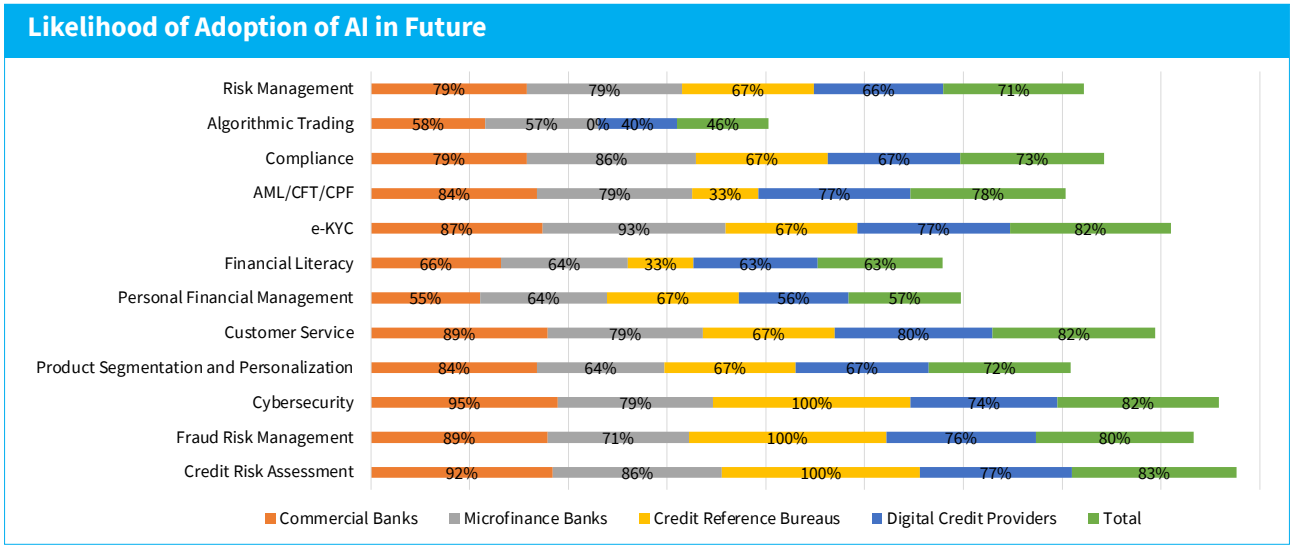

Figure 23: Likelihood of Application of AI in Future

3.3 AI Risk Management

3.3.1 Risks Associated with Usage of AI

- The leading risks reported by institutions that use AI include data quality, governance, and management (59 percent), cybersecurity risks (54 percent), limited numbers of AI-skilled staff (52 percent), third-party dependencies (52 percent) and AI governance risks (51 percent).
- The figures below highlight the overall AI risks reported by institutions and the AI risks per institution type, respectively.

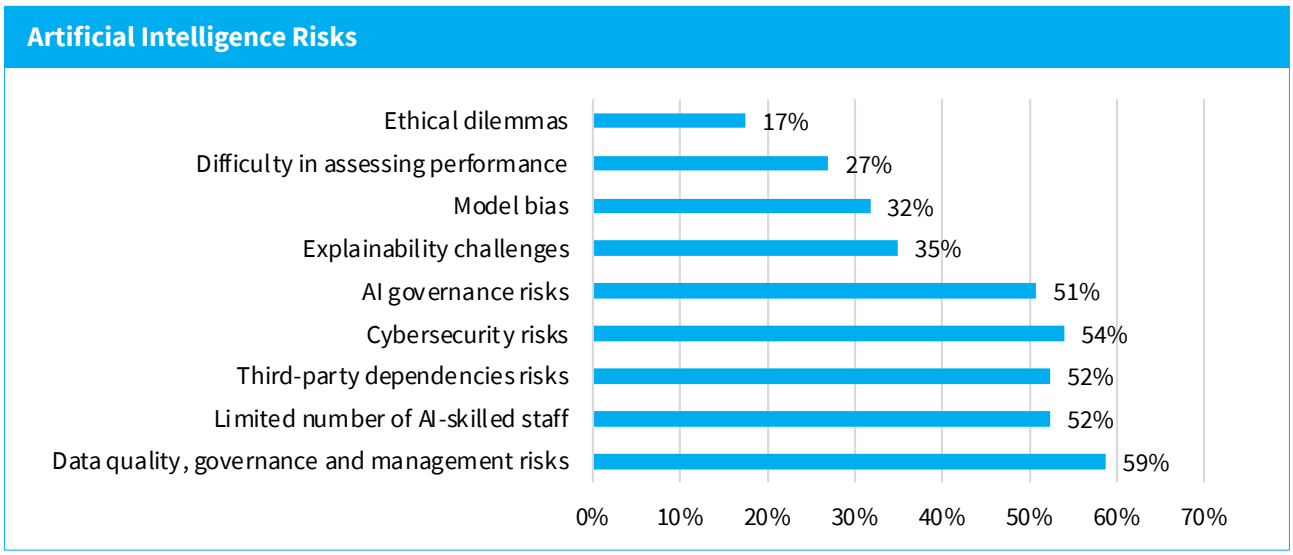

Figure 24: Artificial Intelligence Risks

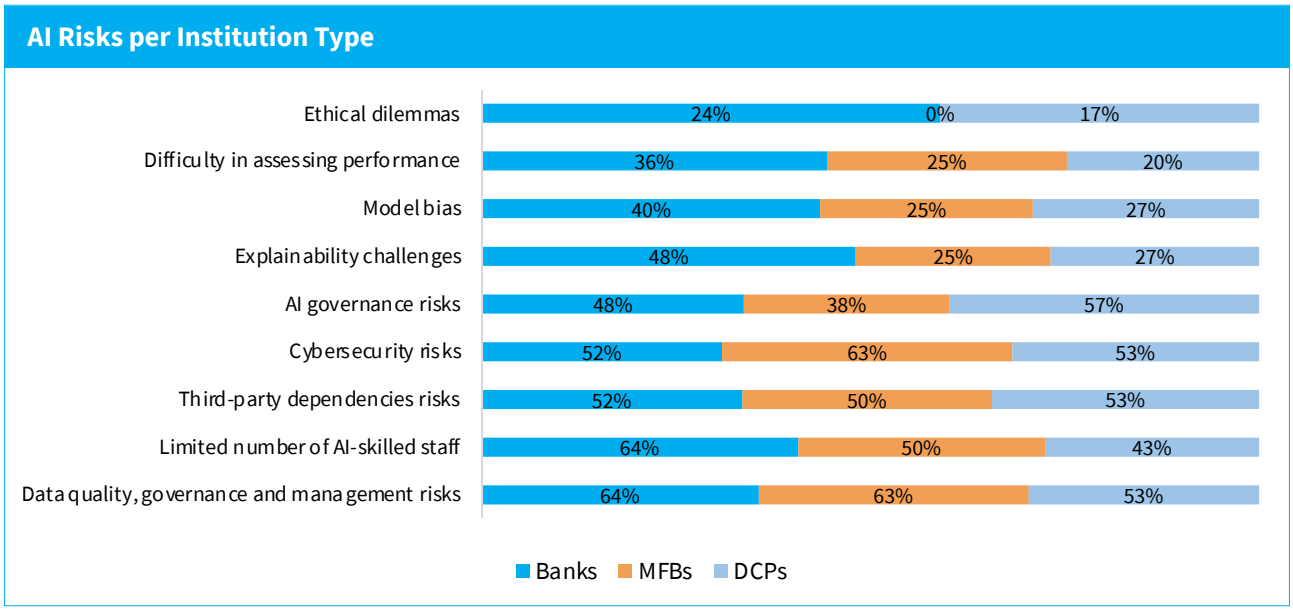

Figure 25: AI Risks per Institution Type

- The measures implemented by institutions to manage the AI/ML model risks included:
  - Implementing policies and practices to ensure data quality, integrity, security, and privacy throughout the AI lifecycle, including regular audits and validation.
  - Establishing AI governance frameworks by defining clear roles, responsibilities, ethical guidelines, and oversight mechanisms to ensure responsible AI development and deployment.
  - Employing techniques and tools to understand AI decision-making processes, as well as enabling human review and intervention where necessary.
  - Implementing measures to identify, assess, and reduce bias in AI models such as using diverse data sets, fairness-aware algorithms, conducting regular audits, and excluding sensitive personal data to avoid discrimination against protected groups.
  - Developing AI expertise by investing in training, upskilling, and hiring skilled AI professionals to build internal capacity to effectively manage AI risks.
  - Addressing third-party dependencies by conducting thorough vetting of AI vendors, establishing clear contractual agreements, and continuously monitoring their performance and security practices.
  - Enforcing cybersecurity measures such as implementing multi-layered security controls, conducting regular vulnerability assessments, and protecting AI systems and data from cyber threats and adversarial attacks.
  - Continuously monitoring and validation of AI model performance through regular testing and retraining to maintain accuracy, reliability, and alignment with evolving business needs and risks.

3.3.2 Measures for Ensuring AI Model Explainability and Transparency for Regulatory Compliance

- 56 percent of the institutions that had adopted AI had put in place measures to ensure the AI models are explainable and not operating as a black box.[5] The institutions comprised 56 percent of commercial banks, 75 percent of MFBs, and 50 percent of DCPs, respectively.
- The measures put in place by institutions to ensure that AI/ML models are explainable included:
  - Use of interpretable models and application of explainability tools to demystify complex models.
  - Implementation of human-in-the-loop mechanisms including override protocols, manual exception handling, and human sampling of outputs.
  - Detailed model documentation outlining the model structure, features, and decision logic.
  - Integration of business rules and expertise in model development and validation.
  - Clear customer communication and transparency.
- Below is a highlight of the proportion of institutions with explainable AI/ML models.

6 A black box is a system which can be viewed in terms of its inputs and outputs (or transfer characteristics), without any knowledge of its internal workings. Source: https://www.cambridge.org/core/journals/philosophy-of-science/article/abs/general-black-box-theory/B7494E2DB8AF8C9C666B67D0DAEDE6E3

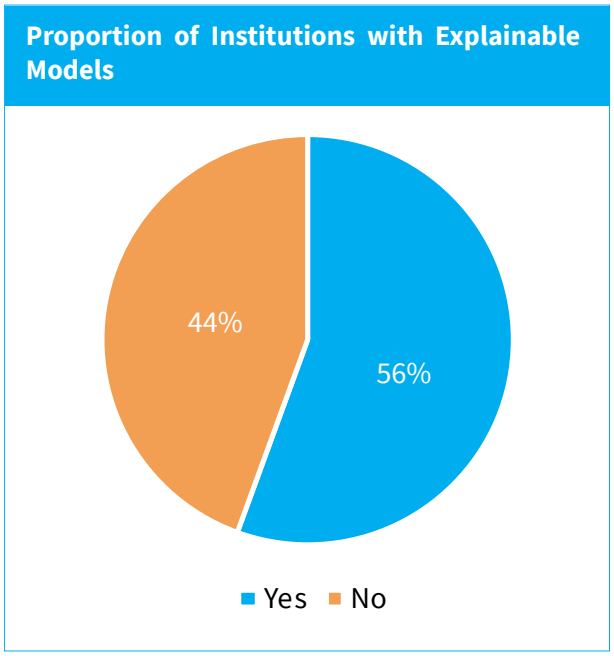

Figure 26: Proportion of Institutions with Explainable Models

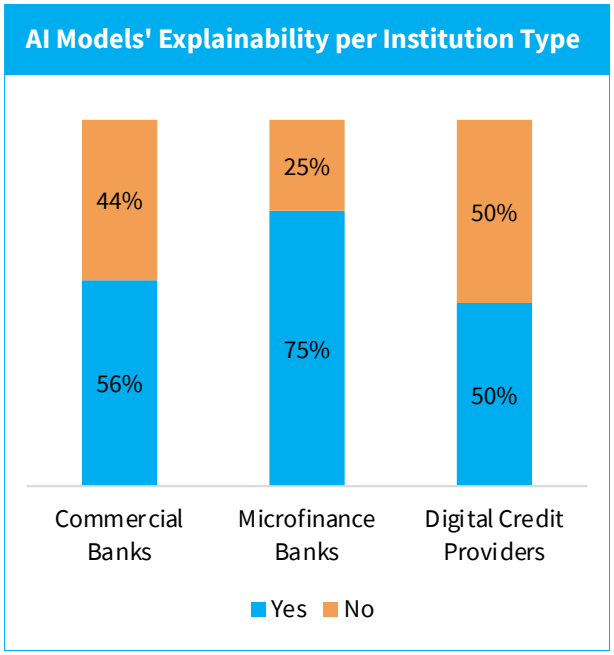

Figure 27: AI Models' Explainability per Institution Type

3.3.3 Access and Equitable Access to AI Models

- The survey sought to establish whether all customers of institutions that had adopted AI had equal access to the benefits of those AI models.
- 73 percent of institutions that had adopted AI customers had equal access to the benefits of the AI models. This included 72 percent of commercial banks, 100 percent of MFBs and 67 percent of DCPs.
- Conversely, 28 percent of commercial banks and 33 percent of DCPs indicated that their models failed to deliver equitable access[6] to their AI models due to design limitations.
- The figures below highlight customer access and equity in implementation of AI models.

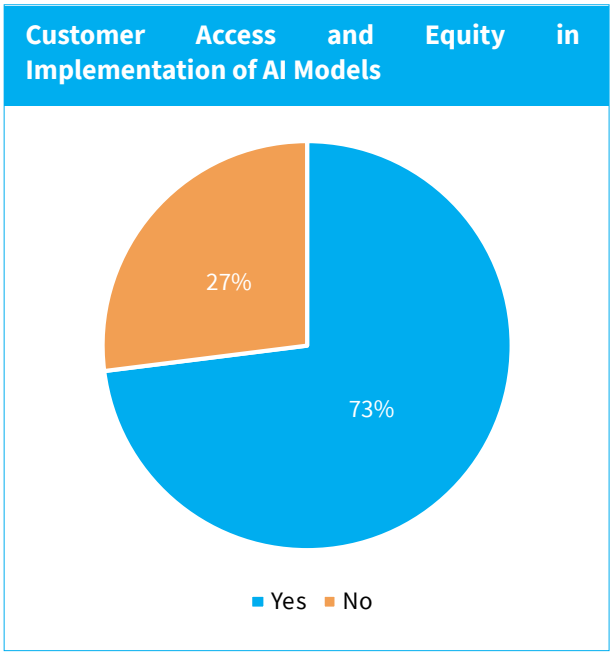

Figure 28: Customer Access and Equity in Implementation of AI Models

6 Equitable access ensures that the advantages of AI technologies are accessible to all individuals and communities, regardless of socioeconomic status, geographic location, or demographic characteristics. https://www.linkedin.com/pulse/empowering-ai-equality-bhojaraja-kumar-p-a-k-a-bhoj--aqrwc#:~:text=Equitable%20access%20to%20AI%20benefits,geographic%20location%2C%20or%20demographic%20characteristics.

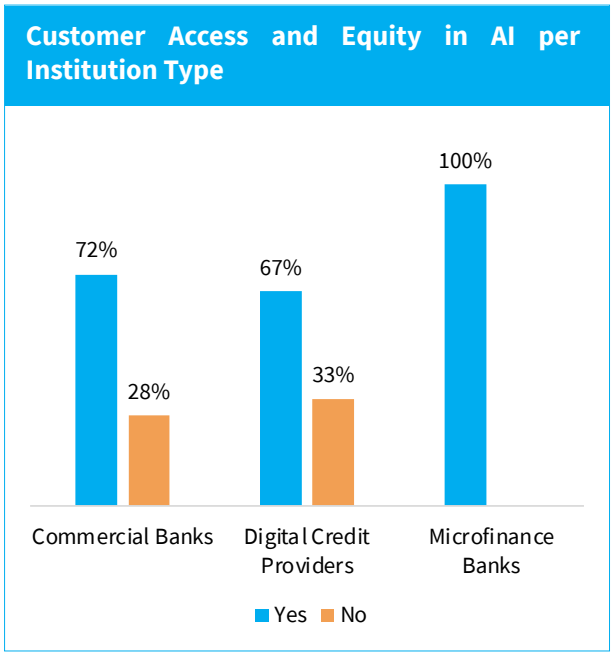

Figure 29: Customer Access and Equity in AI per Institution Type

3.3.4 Anonymization and De-identification of Sensitive Data in ML Model Data Collection and Processing

- 75 percent of respondents had adopted AI anonymized sensitive data used in machine learning models during data collection and processing. The respondents included 84 percent of commercial banks, 88 percent of MFBs and 63 percent of DCPs.
- 86 percent of institutions indicated that users had control of the personal data used in machine learning models, including 80 percent of commercial banks, 100 percent of MFBs and 87 percent of DCPs.

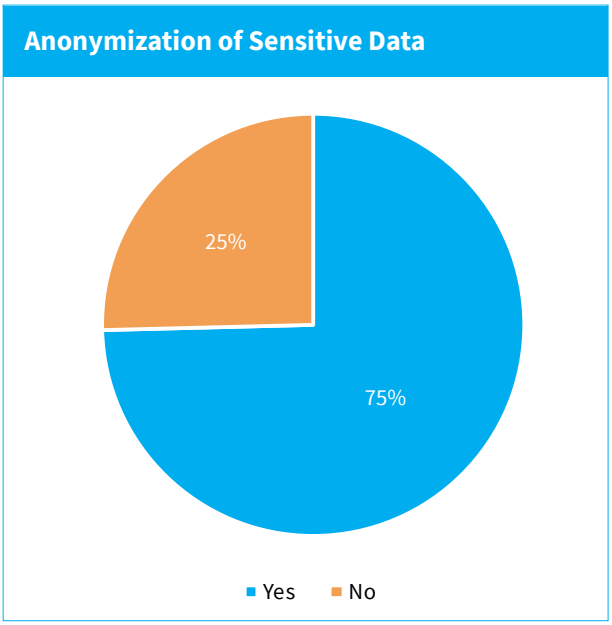

Figure 30: Anonymization of Sensitive Data

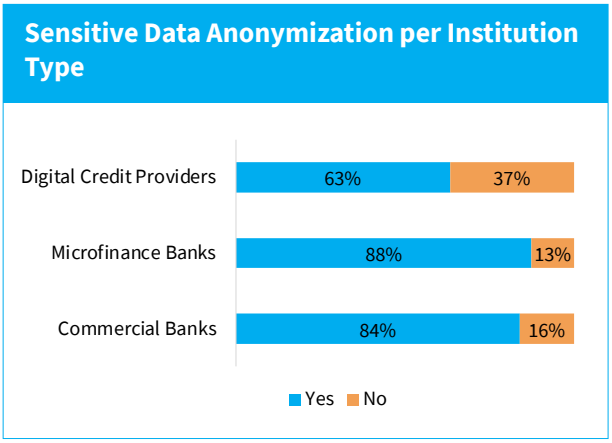

Figure 31: Sensitive Data Anonymization per Institution Type

3.3.5 Mechanisms for Addressing Auditability of Machine Learning Models

- 56 percent of respondents that had adopted the use of AI had mechanisms to address auditability of ML models.
- The mechanisms adopted by institutions to address auditability of ML models included:

- Comprehensive model documentation and version control (tracking model changes, inputs, parameters, and performance metrics).
- Explainability tools, permutation importance, and visualizations to clarify model decisions.
- Human-in-the-loop oversight for high-impact decisions, ensuring manual review and accountability.
- Audit trails and logging, capturing data lineage, predictions, user interactions, and system changes.
- Ongoing model monitoring and drift detection, with alerts to flag performance shifts or biases.
- Internal controls, governance frameworks, and regular internal/external audits to ensure compliance and transparency.
- Adoption of inherently interpretable models.

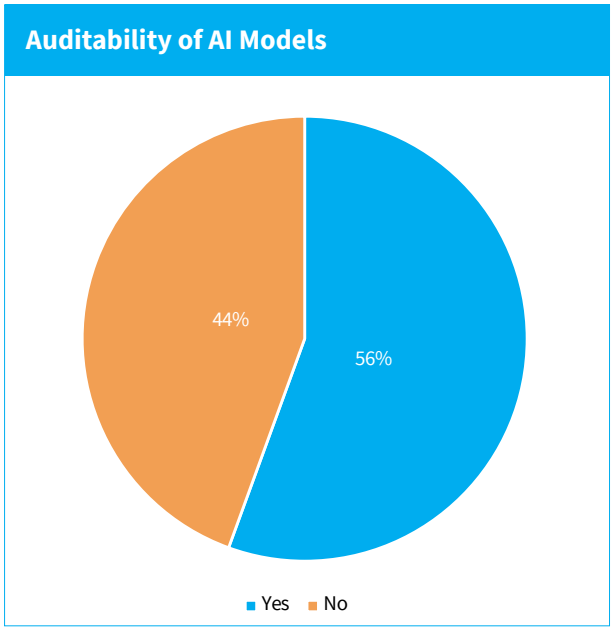

Figure 32: Auditability of AI Models

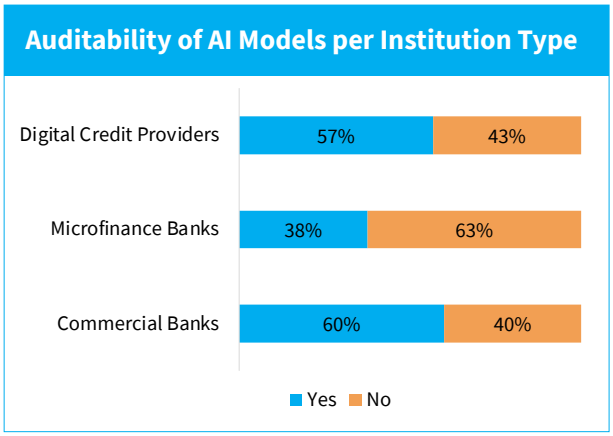

Figure 33: Auditability of AI Models per Institution Type

3.3.6 Mitigating Bias in AI Models

- 62 percent of respondents that were using AI had implemented measures to mitigate bias in AI models. The measures included:
  - Exclusion of Sensitive Attributes such as gender, race, and age from models.
  - Use of datasets that reflect the diversity of the target population to prevent underrepresentation or overrepresentation of specific groups.
  - Regular audits, fairness assessments, and performance monitoring to detect bias.
  - Human-in-the-loop approach where high-stakes decisions or flagged anomalies undergo manual review to ensure fairness.
  - Use of explainability and Fairness Tools to interpret model predictions and assess feature influence, aiding in identifying hidden biases.
  - Internal policies, compliance reviews, and ethical guidelines to mitigate risks of unfair or biased outcomes.

- Use of piloting phases for new models, continuous retraining, and adjustment of datasets or algorithms if bias is detected.
- Training staff on ethical AI practices and involving diverse teams in model development and review processes to enhance bias detection.

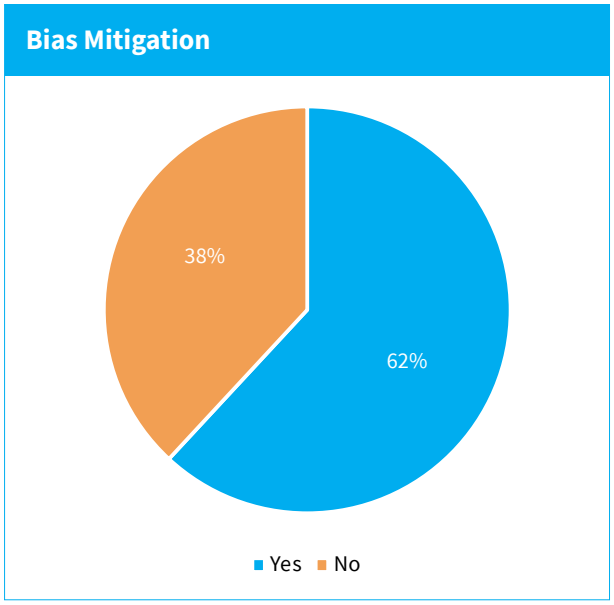

Figure 34: Bias Mitigation

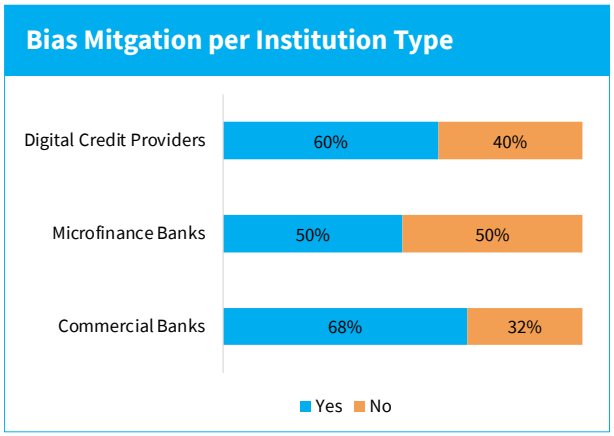

Figure 35: Bias Mitigation per Institution Type

3.3.7 Environmental Impact

- The responses of institutions that acknowledged using Generative Pre-trained Transformer (GPT) or Large Language Models (LLMs), reflect varying degrees of awareness, practical usage patterns, and strategies to mitigate environmental impact. The key themes identified from the institution's responses included:
  - Use of pre-trained models or cloud-based models which limit direct energy consumption and shifts the environmental burden to third-party providers.
  - Adoption of mitigation strategies to minimize environmental footprint including:
    - Fine-tuning rather than training models from scratch to reduce computational demands.
    - Deployment of efficient serving methods to limit Graphics Processing Unit (GPU) usage during inference.
    - Selection of energy efficient AI services and sustainability conscious vendors where possible.

3.4 Impact and Challenges

3.4.1 Impact of AI on Institutional Performance and Operational Efficiency

- 78 percent of institutions that were using AI indicated that AI had enhanced their performance and operational efficiency. This comprised 84 percent of commercial banks, 88 percent of MFBs, and 70 percent of DCPs.

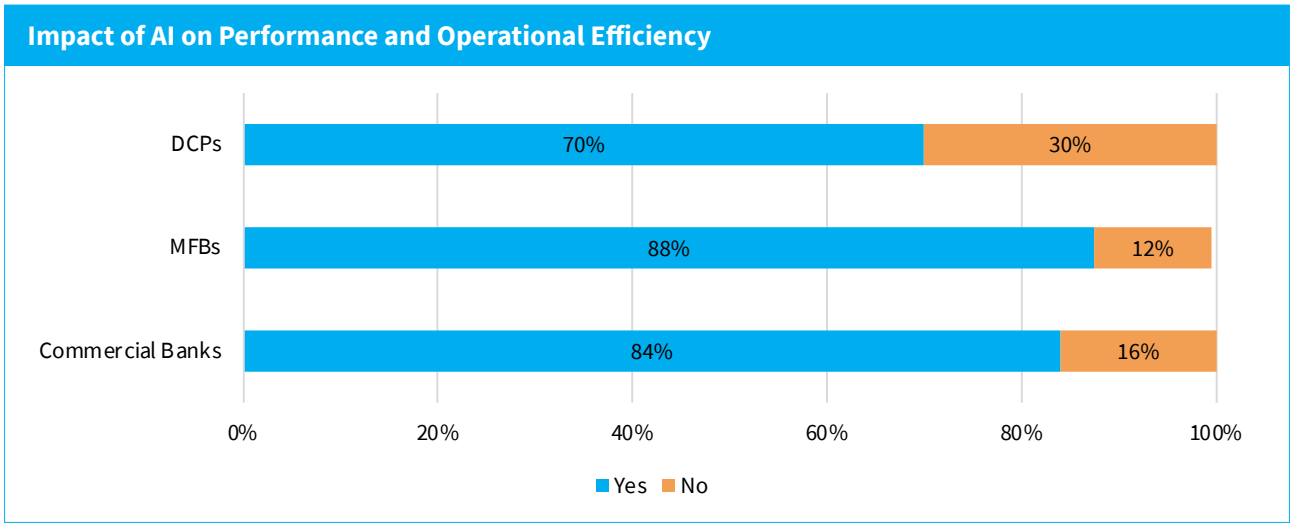

Figure 36: Impact of AI on Performance and Operational Efficiency

- The areas where AI had enhanced performance and operational efficiency included:
  - Operational efficiency improvements leading to faster credit assessment and faster decision-making.
  - Automation of repetitive and manual tasks, such as minute-taking, customer onboarding, and KYC.
  - Improved cybersecurity using AI-driven monitoring tools.
  - Better customer service through automated chats and personalized loan products.
  - Improved accuracy of credit risk assessments, thereby reducing Non-Performing Loans (NPLs).
  - Faster and more proactive fraud detection.
  - Resource optimization through better utilization of staff and systems.

3.4.2 Challenges Faced by Institutions in Adoption of AI

- The top three challenges in the adoption of AI were shortage of skills (46 percent), high costs and limited resources (46 percent), and governance and regulatory compliance challenges (43 percent).
- Institutions that had not implemented AI cited high costs and skills gap as the main reasons for not adopting AI.

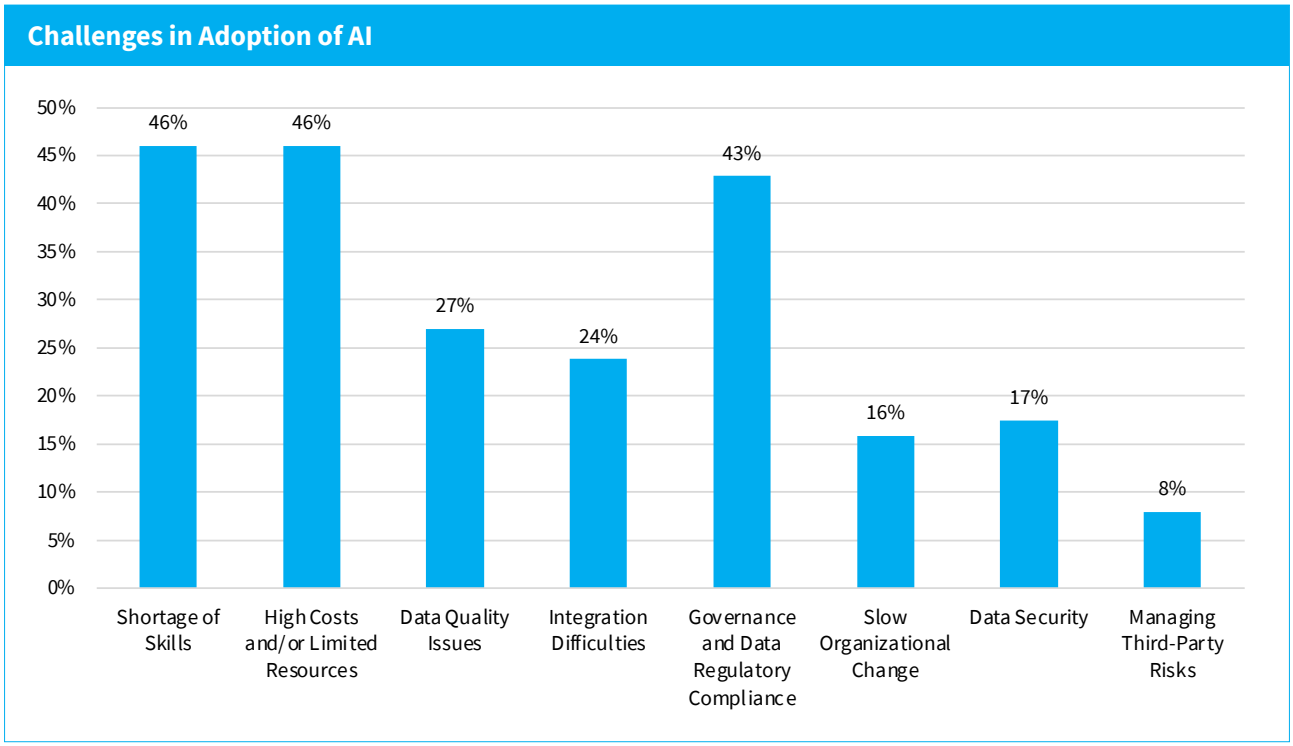

Figure 37: Challenges in Adoption of AI

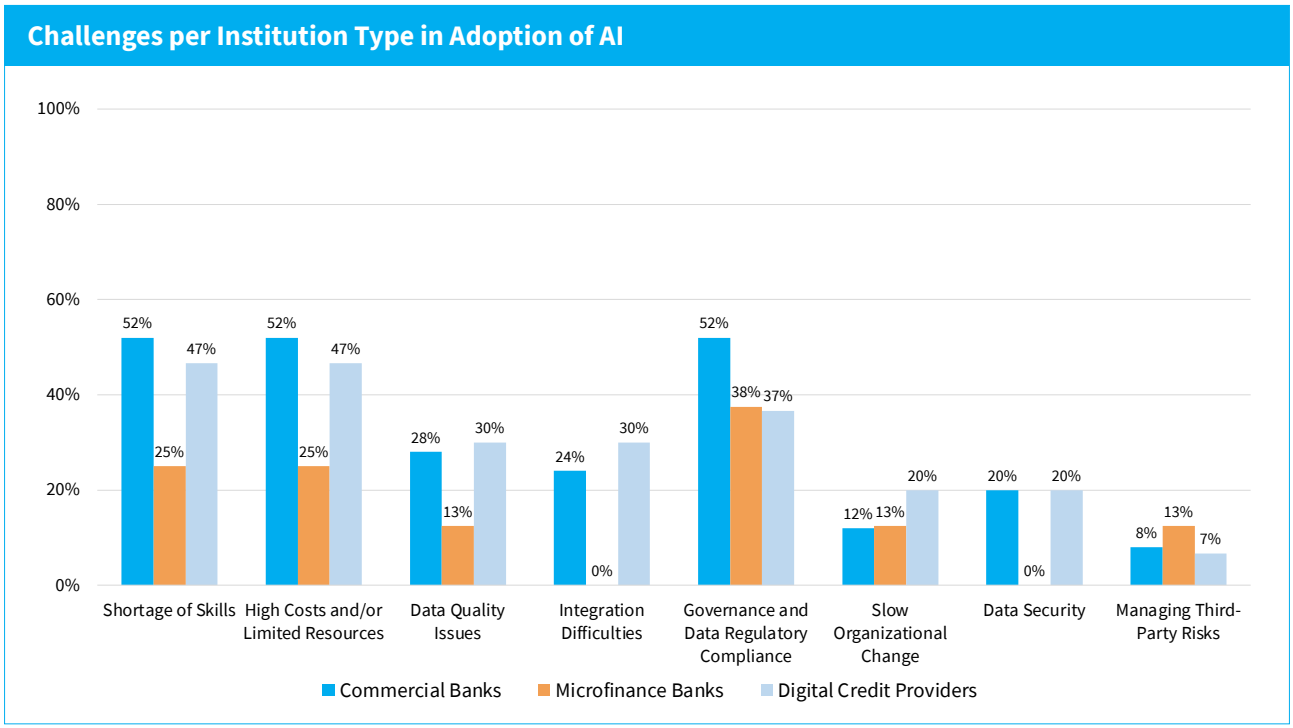

Figure 38: Challenges per Institution Type in Adoption of AI

3.4.3 Monitoring AI/ML Model Performance and Accuracy

- 60 percent of commercial banks, 63 percent of MFBs and 70 percent of DCPs indicated that they had mechanisms to monitor the performance and accuracy of their AI models.

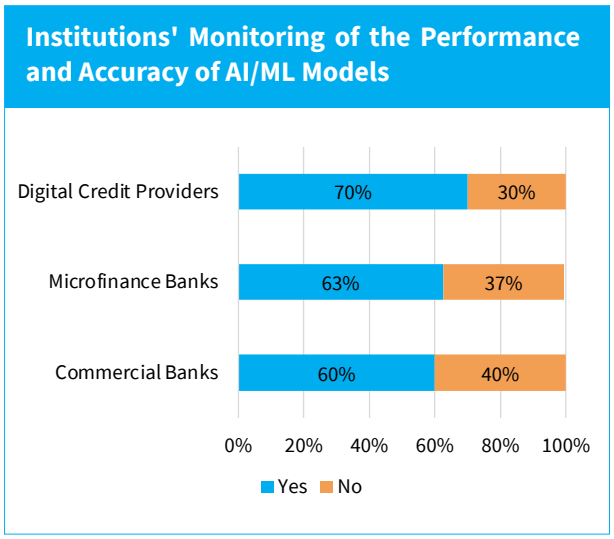

Figure 39: Institutions' Monitoring of the Performance and Accuracy of AI/ML Models

- The methods used for monitoring the performance of AI models included:
  - Tracking present Key Performance Indicators (KPIs) such as accuracy, precision, and recall of ML models.[7]
  - A/B testing[8] of different AI models.
  - Quarterly evaluations.
  - Setting up dashboards and alerts for performance drift.
  - Human reviews for critical decision points.

7 Accuracy measures the proportion of correctly classified instances out of all instances. Precision focuses on the correctness of positive predictions. A high precision means fewer false positives. Recall measures how well the model identifies actual positives. A high recall means fewer false negatives. Source: https://developers.google.com/machine-learning/crash-course/classification/accuracy-precision-recall

8 A/B testing involves comparing two versions of a variable (A and B) to identify which one performs better on a given metric. In the realm of machine learning, these variables often manifest as different models, algorithms, feature sets, or hyperparameters. https://medium.com/@weidagang/demystifying-a-b-testing-in-machine-learning-a923fe07018d s

4.0 Recommendations

- 92 percent of commercial banks,100 percent of MFBs, 100 percent of CRBs and 91 percent of DCPs indicated that CBK should issue guidance on AI to support their AI developments.

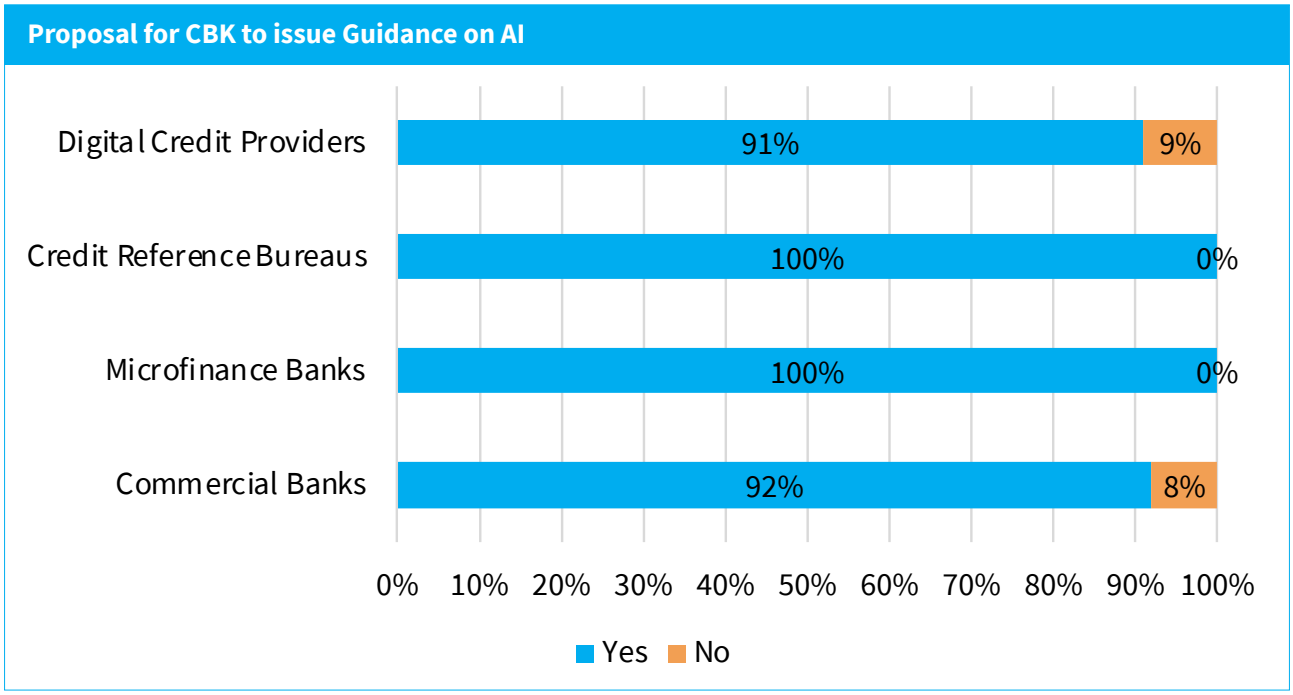

Figure 40: Proposal for CBK to issue Guidance on AI

- The survey respondents proposed the following areas to be covered in the Guidance on AI:
  - **Governance and Compliance:**
    - Data Governance: Ensuring data privacy, security, and ethical handling.
    - Regulatory compliance.
    - Guidance on model transparency, fairness in AI decision-making.
    - Addressing AI bias, discrimination, and promoting ethical AI use.
    - Clarity on use of third-party AI models.
    - Guidance on managing third-party AI vendors.
  - **Risk Management Frameworks:**
    - Accountability structures for AI decisions.
    - Mitigating risks such as bias, unfairness, and lack of transparency.
  - **Incident Management and Reporting:**
    - Clear reporting lines for AI failures.
    - Regulatory reporting requirements.

5.0 Conclusion

The survey report illustrates that institutions have considerable interest in the adoption of AI and will continue to adopt AI to enhance operational efficiency and better serve customers. The adoption of AI has brought about operational efficiencies, particularly in credit risk management, cybersecurity, and customer service. Conversely, institutions face multiple risks as they adopt AI, including bias, inexplicability of models (black box), and challenges in data and AI governance.

A significant portion of the financial institutions reported the implementation of generative AI tools in their operations. This highlights the importance of ensuring that policy efforts cover the impact and risks of generative AI in the banking sector.

As institutions adopt AI, it is necessary for CBK to provide guidance, particularly on best data governance and AI governance strategies, AI risk mitigation measures, and interaction with third-party AI vendors. Accordingly, CBK has embarked on the process of developing guidance on AI for the banking sector.

Annex 1: Glossary of Terms

AI Policy	A guiding framework for organizations, delineating the principles, guidelines, and procedures governing the deployment and use of AI systems.
AI Strategy	A comprehensive plan that serves as a roadmap outlining how an organization will leverage AI to achieve its business objectives.
Algorithm	A sequence of rules given to an AI machine to perform a task or solve a problem. Common algorithms include classification, regression, and clustering.
Artificial Intelligence	Simulation of human intelligence in machines programmed to perform tasks that typically require human intelligence.
Artificial Intelligence Platform	An integrated collection of technologies to develop, train, and run machine learning models.
Bias	Output errors caused by skewed training data in AI Models.
Big Data	Extremely large and diverse collections of structured, unstructured, and semi-structured data that continues to grow exponentially over time.
Business Intelligence	A set of technological processes for collecting, managing, and analysing organizational data to yield insights that inform business strategies and operations.
Cloud Computing Platforms	Refers to the operating system and hardware of a server in an Internet-based data centre. It allows software and hardware products to co-exist remotely and at scale.
Collaboration and Version Control Tools	Essential tools used in software development and collaborative projects to track and manage changes to code, documents, and other files.
Data Analytics	The process of analysing raw data to draw out meaningful, actionable insights.
Data Strategy	A comprehensive blueprint guiding the processes, policies, and technologies for data collection, storage, management, and analysis across every area of the business.
Data Visualization	A comprehensive long-term plan defining data collection, storage, sharing, and utility while aligning with the institution's business strategy.

Development Operations (DevOps)	A software development methodology that accelerates the delivery of high-performance applications and services by combining and automating the work of software development (Dev) and IT operations (Ops) teams.
Graphics Processing Unit (GPU)	A specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images and videos. While originally designed for graphics rendering, GPUs are now widely used in various applications like gaming, content creation, and AI, due to their ability to perform massive parallel calculations.
Hybrid AI	Any artificial intelligence technology that combines multiple AI methodologies.
Human-in-the-Loop Mechanism	A collaborative approach that integrates human input and expertise into the lifecycle of machine learning (ML) and artificial intelligence systems.
Large Language Model (LLM)	A statistical language model, trained on a massive amount of data, that can be used to generate and translate text and other content, and perform other natural language processing (NLP) tasks.
Machine learning (ML)	A subset of artificial intelligence that focuses on building systems that learn and improve as they consume more data.
Machine Learning Model	Computer programs that are used to recognize patterns in data or make predictions.
Machine Learning Operations (MLOps)	A set of practices designed to create an assembly line for building and running machine learning models.
Machine Learning Platform	Provides a robust and scalable infrastructure that enables organizations to harness the potential of their data and apply advanced algorithms to uncover patterns, trends, and predictions.
Parameters	A set of numerical weights representing neural connections or other aspects in an AI model with values that are determined by training.
Synthetic Data	Artificial data that is generated from original data and a model that is trained to reproduce the characteristics and structure of the original data.

Annex 2: Bibliography

1. Central Bank of Kenya. (2024). Banking Sector Innovation Survey 2024. Retrieved from https://www.centralbank.go.ke/uploads/banking_sector_reports/1736029340_Banking%20Sector%20Innovation%20Survey%202024.pdf
2. Gartner. (2020). Artificial Intelligence Maturity Model. Retrieved from https://www.gartner.com/en/documents/3982174
3. Bunge, M. (1963). A general black box theory. Philosophy of Science, 30(4), 346–358. Retrieved from https://www.cambridge.org/core/journals/philosophy-of-science/article/abs/ general-black-box-theory/B7494E2DB8AF8C9C666B67D0DAEDE6E3
4. Kumar, B. (2024). Empowering AI equality: Equitable access to AI benefits. Retrieved from https://www.linkedin.com/pulse/empowering-ai-equality-bhojaraja-kumar-p-a-k-a-bhoj--aqrwc#:~:text=Equitable%20access%20to%20AI%20benefits,geographic%20location%2C%20or%20demographic%20characteristics
5. Google Developers. (2024). Classification: Accuracy, recall, precision, and related metrics. Retrieved from https://developers.google.com/machine-learning/crash-course/classification/accuracy-precision-recall
6. Lindemulder, G., & Kosinski, M. (2025). DevOps. IBM. https://www.ibm.com/think/topics/devops
7. Mucci, T., & Stryker, C. (2025s). MLOps. IBM. https://www.ibm.com/think/topics/mlops
8. Weidagang, W. (2024). Demystifying A/B testing in machine learning. Retrieved from https://medium.com/@weidagang/demystifying-a-b-testing-in-machine-learning-a923fe07018d

Annex 3: List of Respondents

a. Commercial Banks and Mortgage Finance Institution

1. Absa Bank Kenya Plc.
2. Access Bank (Kenya) Plc.
3. African Banking Corporation Limited.
4. Bank of Africa Kenya Limited.
5. Bank of Baroda (Kenya) Limited.
6. Bank of India.
7. Citibank N.A. Kenya
8. Consolidated Bank of Kenya Limited.
9. Co-operative Bank of Kenya Limited.
10. Credit Bank Plc.
11. Development Bank of Kenya Limited.
12. Diamond Trust Bank Kenya Limited.
13. DIB Bank Kenya Limited.
14. Ecobank Kenya Limited.
15. Equity Bank Kenya Limited
16. Family Bank Limited.
17. First Community Bank Limited.
18. Guaranty Trust Bank (Kenya) Limited.
19. Guardian Bank Limited.
20. Gulf African Bank Limited.
21. Habib Bank A.G Zurich.
22. HFC Limited.
23. I&M Bank Limited.
24. KCB Bank Kenya Limited.
25. Kingdom Bank Limited.
26. Mayfair CIB Bank Limited.
27. Middle East Bank Kenya Limited.
28. M-Oriental Bank Limited.
29. National Bank of Kenya Limited.
30. NCBA Bank Plc.
31. Paramount Bank Limited.
32. Prime Bank Limited.
33. SBM Bank Kenya Limited.
34. Sidian Bank Limited.
35. Stanbic Bank Kenya Limited.
36. Standard Chartered Bank Kenya Limited.
37. UBA Kenya Bank Limited.
38. Victoria Commercial Bank Limited.

b. Microfinance Banks

1. Branch Microfinance Bank Limited.
2. Caritas Microfinance Bank Limited.
3. Choice Microfinance Bank Limited.
4. Daraja Microfinance Bank Limited.
5. Faulu Microfinance Bank Limited.
6. Kenya Women Microfinance Bank Plc.
7. LOLC Microfinance Bank Plc.
8. Maisha Microfinance Bank Ltd.
9. Muungano Microfinance Bank Plc
10. Rafiki Microfinance Bank Limited.
11. Salaam Microfinance Bank Limited.
12. SMEP Microfinance Bank Limited.
13. Sumac Microfinance Bank Limited.
14. U & I Microfinance Bank Limited.

c. Credit Reference Bureaus

1. Credit Reference Bureau Africa Limited (Trading as TransUnion).
2. Creditinfo Credit Reference Bureau Kenya Limited.
3. Metropol Credit Reference Bureau Limited.

d. Digital Credit Providers

1. Ambush Capital Limited.
2. Anjoy Credit Limited.
3. Asante FS East Africa Limited.
4. Autochek Limited.
5. Azura Credit Limited.
6. Bytech Credit Limited.

7. Ceres Tech Limited.
8. Chelete Credit Limited.
9. Chime Capital Limited.
10. Colkos Enterprises Limited.
11. Creditarea Capital Limited.
12. Decimal Capital Limited.
13. Dime Credit Limited.
14. ED Partners Africa Limited.
15. EDOMX Limited.
16. Ellegant Credit Limited.
17. Extend Money Services Limited.
18. Factorhouse Limited.
19. Fahari Point Capital Limited.
20. Fincorp Credit Limited.
21. Fortune Credit Limited.
22. Fourth Generation Capital Limited.
23. Getcash Capital Limited.
24. Giando Africa Limited (Trading as Flash Credit Africa).
25. Hela Capital Limited.
26. Inspire Credit Limited.
27. Inventure Mobile Limited (Trading as Tala).
28. Ismuk Credit Limited.
29. Jijenge Credit Limited.
30. Jumo Kenya Limited.
31. Kweli Smart Solutions Limited.
32. Lenana Innovative Solutions Limited.
33. Letshego Kenya Ltd.
34. Lipa Later Limited.
35. Little Pesa Limited.
36. LockBx Limited.
37. Maralal Ledger Limited.
38. Marble Capital Solutions Limited.
39. MCF 2 Kenya Limited.
40. Mint Credit Limited.
41. MKM Capital Limited.
42. M-Kopa Loan Kenya Limited.
43. Mogo Auto Limited.
44. Momentum Credit Limited.
45. MyWagepay Limited.
46. Ngao Credit Limited.
47. ODI Credit Limited.
48. Opal Quick Limited.
49. Payablu Credit Limited.
50. Pesaglow Capital Limited.
51. Pezesha Africa Limited.
52. Phoenix Capital Limited.
53. Premier Credit Limited.
54. Progressive Credit Limited.
55. Puphik Credit Limited.
56. Rewot Ciro Limited.
57. Risine Credit Limited.
58. Sevi Innovation Limited.
59. Simplepay Capital Limited.
60. Siti Mobility Technologies Limited.
61. Sokohela Limited.
62. Stride Credit Limited.
63. Tanir Credit & Accounting Services Limited.
64. Tenakata Enterprises Limited.
65. Tip-Point Capital Limited.
66. Treasure Store Limited.
67. Umoja Fanisi Limited.
68. Zanifu Limited.
69. Zenka Digital Limited.
70. Zillions Credit Limited.

Central Bank of Kenya

Haile Selassie Avenue P.O. Box 60000 - 00200 Nairobi |Tel: (+254) 20 - 286 0000 / 286 1000 / 286 3000

www.centralbank.go.ke | www.facebook.com/CentralBankKenya | @CbkKenya