



**DRAFT GUIDANCE NOTE ON ARTIFICIAL INTELLIGENCE IN THE
BANKING SECTOR**

AUGUST 2026

TABLE OF CONTENTS

PART I: PRELIMINARY	3
1.1 Title.....	3
1.2 Application	3
1.3 Authorization	3
1.4 Definitions	3
PART II: STATEMENT OF POLICY	4
2.1 Purpose	4
2.2 Scope	5
2.3 Responsibility	5
2.4 Kenya National Artificial Intelligence Strategy	5
2.5 Overview of Artificial Intelligence in the Banking Sector.....	6
PART III: LEGAL AND REGULATORY REQUIREMENTS.....	7
3.1 Data Protection Act, 2019	8
3.2 Consumer Protection Act.....	9
PART IV: SPECIFIC REQUIREMENTS	9
4.1 Governance Framework	9
4.1.1 Role of the Board of Directors	9
4.1.2 Role of Senior Management.....	12
4.2 Role of Risk Management Function.....	13
4.3 Independent Audit and Assessment.....	13
4.4 Principles of Ethical and Responsible use of Artificial Intelligence	14
4.4.1 Customer-centricity	14
4.4.2 Ethics	14
4.4.3 Fairness and Responsibility.....	14
4.4.4 Transparency and Explainability	14
4.4.5 Privacy and Security.....	14
4.4.6 Continuous Monitoring	15
4.4.7 Learning and Development	15
4.5 Data Governance	15
4.6 AI Risk Management Life Cycle.....	16

4.6.1	Risk Identification	16
4.6.2	Risk Assessment and Classification	17
4.6.3	Risk Mitigation and Control.....	17
4.6.4	Risk Monitoring	17
4.6.5	Risk Reporting and Escalation	17
4.6.6	Periodic Review and Continuous Improvement.....	17
4.6.7	Documentation and Record Keeping	18
4.7	AI System Life Cycle	18
4.8	Model Risk Management	20
4.9	Third-Party AI Risk Management	20
4.10	Generative AI.....	21
4.11	Agentic AI	21
4.12	AI Incident Management.....	22
4.13	Documentation and Record Keeping	23
4.14	Training and Awareness.....	23
4.15	Consumer Protection and Market Conduct	23
4.15.1	Disclosure Obligations	23
4.15.2	Human Review for Critical Decisions.....	24
4.15.3	Complaints Redress Mechanisms.....	25
PART V: REPORTING		25
ANNEX I: High-Level Contents of a Data Governance Policy		27
ANNEX II: High-Level Contents of an Artificial Intelligence Policy		30
ANNEX III: Data Governance and Artificial Intelligence Checklist		32
ANNEX IV: Artificial Intelligence Deployment Register (Annual)		38
ANNEX V: Artificial Intelligence Incident Record (Immediate).....		39
ANNEX VI: Artificial Intelligence Incident Record (Final)		40
ANNEX VII: Artificial Intelligence Incident Record (Quarterly).....		42
REFERENCES.....		43

PART I: PRELIMINARY

1.1 Title - Guidance Note on Artificial Intelligence.

1.2 Application - This Guidance Note applies to:

- i) All institutions licensed under the Banking Act (Cap. 488).
- ii) All institutions licensed under the Microfinance Act (Cap. 493C).
- iii) Credit Reference Bureaus, Money Remittance Providers, and Non-deposit-taking Credit Providers licensed under the Central Bank of Kenya Act (Cap. 491).
- iv) Non- Operating Holding Companies (NOHCs),

The institutions are herein collectively referred to as “financial institutions” or “institutions”.

1.3 Authorization - This Guidance Note is issued under Section 57 (1) of the Central Bank of Kenya Act, Section 33(4) of the Banking Act, Section 48(2A) of the Microfinance Act, and which empowers the Central Bank of Kenya (CBK) to issue guidelines to be adhered to by institutions in order to carry out the objects of the Central Bank of Kenya Act, maintain a stable and efficient banking system, and maintain a stable and efficient deposit-taking microfinance system, respectively.

1.4 Definitions - The terms and acronyms used in this Guidance Note are defined below:

- 1.4.1 “Artificial Intelligence agents (AI agents)”** means systems designed to act autonomously, making decisions and taking actions based on their programming and objectives. These systems are capable of performing tasks without constant human intervention.
- 1.4.2 “Agentic Artificial Intelligence (Agentic AI)”** means an artificial intelligence system that is capable of autonomously planning, making decisions and executing actions in pursuit of defined objectives with limited human intervention.
- 1.4.3 AI Incident”** means events where AI models produce harmful, biased, or unintended outcomes, degrade materially in performance, or are compromised.
- 1.4.4 “Algorithm”** means a sequence of rules given to an AI machine to perform a task or solve a problem. Common algorithms include classification, regression, and clustering.
- 1.4.5 “Artificial Intelligence (AI)”** means a simulation of human intelligence in machines programmed to perform tasks that typically require human intelligence.
- 1.4.6 “Bias”** means output errors caused by skewed training data in AI models.

- 1.4.7 “Critical AI system”** means an AI system that supports an institution’s services where disruption of the AI system would significantly impact financial stability, customer confidence, or regulatory obligations.
- 1.4.8 “Critical decision”** means an AI-driven outcome that has a significant legal, financial, or similarly substantive effect on a customer. This includes, but is not limited to, credit denial, fraud flagging, account freezing, and pricing adjustments.
- 1.4.9 “Digital redlining”** means the practice of creating and perpetuating inequities between already marginalized groups through the use of digital technologies, digital content, and the internet.
- 1.4.10 “Explainability”** means the ability to understand and articulate, in clear and simple terms, how an AI model makes its decisions and the factors influencing those decisions.
- 1.4.11 “Generative AI”** means a subset of AI that produces new content, such as text, images, audio or video, based on patterns learned from existing data or training data, usually in response to a user’s prompt.
- 1.4.12 “Incident”** means an event that disrupts or threatens to disrupt institutions’ operations, customer service, regulatory compliance, or data security.
- 1.4.13 “Machine Learning (ML)”** means a subset of artificial intelligence that focuses on building systems that learn and improve as they consume more data.
- 1.4.14 “Machine Learning Model”** means computer programs that are used to recognize patterns in data or make predictions.
- 1.4.15 “Model Hallucination” or “Confabulation”** means the production of confidently stated but erroneous or false content by which users may be misled or deceived.
- 1.4.16 “Parameters”** means a set of numerical weights representing neural connections or other aspects in an AI model with values that are determined by training.
- 1.4.17 “Relevant incident”** means incidents that significantly affect critical systems, disrupt services, or compromise data integrity, requiring notification to Central Bank of Kenya.
- 1.4.18 “Synthetic data”** means artificial data that is generated from original data and a model that is trained to reproduce the characteristics and structure of the original data.

PART II: STATEMENT OF POLICY

2.1 Purpose

This Guidance Note outlines the minimum requirements for the safe, ethical, and responsible adoption of AI by financial institutions. The Guidance Note aims to: -

- a) Promote ethical and responsible use of artificial intelligence by financial institutions.
- b) Strengthen financial stability and foster public trust and confidence in the financial system by mitigating operational, systemic, cybersecurity, and market risks associated with AI systems.
- c) Ensure fairness, ethics, and accountability in AI-driven decisions.
- d) Safeguard consumers from unfair, discriminatory, opaque, or harmful AI-driven decisions and practices.
- e) Establish governance, accountability, risk management, and human oversight expectations for AI systems used by institutions in financial services.
- f) Provide supervisory clarity on the use of AI for financial services.
- g) Address emerging AI-related risks such as algorithmic bias, data privacy breaches, cyber threats, model hallucinations, lack of explainability, autonomous decision-making risks.
- h) Foster responsible innovation, enhance efficiency, and support the development of robust AI solutions within the financial sector.

2.2 Scope

This Guidance Note sets out minimum expectations for the safe, ethical, and responsible adoption of AI in the conduct of banking business and the provision of financial services. It shall be applicable when an institution develops and implements AI, or relies on third parties for AI systems, processes, and functions. It is not a replacement for and does not supersede the legislation, regulations and guidelines that institutions must comply with as part of their regulatory obligations, particularly in the areas of risk management, outsourcing, information communication technology, internal controls and corporate governance.

2.3 Responsibility

The Board of Directors of financial institutions bear the primary responsibility for ensuring ethical and responsible adoption of AI by financial institutions. This includes establishing appropriate governance structures and risk management frameworks to safeguard institutional resilience.

2.4 Kenya National Artificial Intelligence Strategy

The Kenya Artificial Intelligence Strategy 2025-2030¹ was launched on March 27, 2025. The strategy aims to harness the transformative potential of AI to drive the country's socioeconomic development. The strategy serves as a roadmap to position Kenya as an

¹ <https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf>

African leader in AI by creating an action plan for a robust, inclusive, and sustainable AI-driven future.

The strategy outlines the strategic decisions, guiding principles, and priority areas for AI development, while considering the diverse needs and perspectives of Kenyans. Key AI policy directions include:

- **AI Digital Infrastructure:** Developing a robust digital infrastructure.
- **Data:** Establishing a strong data governance framework.
- **Research and Development:** Fostering AI research and development.
- **Talent:** Prioritizing AI talent development.
- **Governance:** Implementing agile governance and regulatory structures.
- **Investment:** Encouraging public and private sector investments.
- **Ethics, Equity, and Inclusion:** Promoting ethical, equitable, and inclusive AI practices.

The strategy acknowledges the role of AI in the financial sector, particularly in promoting financial inclusion and access to credit. Additionally, the strategy acknowledges the Central Bank of Kenya as a key stakeholder for involvement in policy and other decisions. Further, the strategy recognizes the importance of managing risks associated with AI, such as cybersecurity threats, data privacy, and data governance concerns. This is similar to CBK's innovation philosophy of maximizing the benefits of innovation while minimizing their risks. Accordingly, CBK's focus on AI aligns with the national strategy's objective to integrate AI into key sectors, including finance.

2.5 Overview of Artificial Intelligence in the Banking Sector

Advances in digital technology and data analytics have led to increased adoption of AI in financial services globally. AI presents opportunities for enhancing efficiency, improving risk management, and deepening financial inclusion. AI technologies are increasingly being adopted across the Kenyan banking sector to improve operational efficiency, customer service, and risk management. However, AI also introduces new risks, including model bias, data privacy concerns, cyber risk vulnerabilities, and challenges related to transparency and accountability.

In recognition of the rising importance of AI, CBK conducted a survey² on the use of AI in the banking sector in 2025. The survey targeted commercial banks, mortgage finance institutions, Credit Reference Bureaus (CRBs), Microfinance Banks (MFBs) and Digital Credit Providers (DCPs). The Survey sought to assess the adoption of AI among financial

² https://www.centralbank.go.ke/uploads/banking_sector_reports/595566510_Survey%20on%20Artificial%20Intelligence%20in%20the%20Banking%20Sector.pdf

institutions, understand key benefits, risks, and mitigation strategies and gather insights for policy development. Key findings are summarized below:

- i) **Adoption:** 50 percent of all surveyed institutions indicated they had adopted AI solutions. This comprised 66 percent of commercial banks, 57 percent of MFBs, and 43 percent of DCPs. All CRBs indicated non-adoption of AI in their operations. Most of the institutions which had not adopted AI were exploring the potential use of AI in their institutions.
- ii) **Strategy and Governance:** 30 percent of institutions had formal AI strategies while 62 percent had data strategies and dedicated data/AI teams. Institutions with AI strategies cited use cases such as credit scoring, fraud detection, and customer support chatbots.
- iii) **Applications of AI in the Banking Sector:** The top three applications of AI and ML in the banking sector were credit risk assessment (65 percent), cybersecurity (54 percent), and customer service (43 percent). Notably, 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 electronic Know-your-Customer (e-KYC) solutions.
- iv) **Risk Management:** Common risks identified included data quality, governance challenges, cybersecurity risks, and third-party dependencies.
- v) **Challenges:** The challenges in implementing AI included limited AI-skilled staff, high costs of AI, and data and governance regulatory compliance challenges.
- vi) **Impact:** AI has enhanced operational efficiency, improved decision-making, and enabled new financial products.
- vii) **Recommendations from Institutions:** 93 percent of respondents recommended that CBK issues a comprehensive Guidance on AI, covering governance and compliance, risk management, and incident management and reporting.

In view of these developments, CBK has issued this Guidance Note to financial institutions to entrench ethical and responsible use of AI and strengthen supervisory oversight over the use of AI by institutions. The Guidance Note outlines CBK's expectations for responsible AI deployment, balancing the benefits of innovation with the need for prudential soundness and protection of financial sector stakeholders. The Guidance Note has been developed in line with best practices by standard-setting bodies as well as practices in leading and comparative jurisdictions.

PART III: LEGAL AND REGULATORY REQUIREMENTS

Institutions should comply with all legal and regulatory requirements, in addition to those outlined below, which are useful in AI undertakings.

3.1 Data Protection Act, 2019

The Data Protection Act, 2019, establishes the legal framework for data processing activities and the protection of personal data in Kenya. Below are critical considerations for financial institutions (FIs) adopting Artificial Intelligence (AI) to ensure compliance with the Act.

- **Assess the use of AI** – Institutions should assess how they will use AI across the business and establish a lawful basis for doing so.
- **Register as a data controller and data processor** – Institutions are required to register as a data controller and/or data processor.
- **Appoint a Data Protection Officer** - Institutions should designate or appoint a data protection officer.
- **Respect the rights of data subjects.** The Act outlines the rights of individuals; these include:
 - Right to be informed – Institutions should be clear and transparent about what data they are collecting.
 - Right to Access – personal data in custody of data controller or data processor.
 - Right to Object – object to processing of all or part of their personal data.
 - Right to correct false or misleading data.
 - Right to delete false or misleading data about them.
- **Data Protection Impact Assessments** – the Data Protection Act 2019, requires institutions to conduct impact assessments where a data processing operation is deemed to be high risk or is likely to infringe on the rights and freedoms of a data subject. It is also important to maintain an audit mechanism of the system to track the factors affecting the decisions being generated.
- **Consent** – Institutions are required to fulfil the consent requirement before processing personal data. Consent must be informed, explicit, and given freely. The data subject may also withdraw their consent at any time.
- **Disclose specified purpose of data collection** - the purpose for which data is collected must also be made explicit. The Act states that data must only be collected for its intended purpose and prohibits the reuse of data beyond the original scope of collection.
- **Automated Decisions** - The Data Protection Act sets out rules for automated decision making. It emphasizes that such decisions must be subject to appropriate safety measures. Data subjects have the right to request human review of decisions, express their own view and contest any decision if necessary.

- **Disclosure of data to third parties** - Disclosure of personal data to a third party without prior authority of the data controller or data processor is an offense.
- **Complaints** – Institutions should establish complaints redress mechanisms to address data-related complaints.

3.2 Consumer Protection Act

The Consumer Protection Act, 2012, provides for the protection of consumers, prevention of unfair trade practices and regulation of consumer transactions. Below are some considerations for institutions using AI systems:

- **Fairness and Non-Discrimination** – AI-based decisions should not result in unfair, unreasonable, or discriminatory treatment. Algorithmic bias should be closely monitored, and institutions should implement mechanisms to mitigate it.
- **Right to Redress** – Consumers have a right to seek redress if an AI decision impacts them negatively. They also have the right to an explanation and an opportunity to challenge it. Institutions should establish channels through which customers can raise complaints.

PART IV: SPECIFIC REQUIREMENTS

4.1 Governance Framework

4.1.1 Role of the Board of Directors

The board of directors holds the ultimate responsibility for and guiding the ethical development and use of AI in their institutions. They are responsible for formulating the institution's data governance and AI frameworks, strategies, and policies.

Data governance is the foundation of AI, given that AI is heavily dependent on data. The relationship between data governance and AI is outlined below.

- The Data Governance Strategy establishes the enterprise-wide approach to managing data.
- The Data Governance Policy translates the Data Governance Strategy into mandatory requirements.
- a) The Data Governance Framework provides the mechanisms and controls to implement the Data Governance Strategy and Policy and defines how the institution collects, manages, secures, and stores data. The data governance framework should also outline standards for data management in the institution.

- The AI Strategy builds upon the overarching data governance foundation by determining how the institution will adopt and derive value from AI.
- The AI Policy establishes the mandatory requirements for responsible use of AI.
- The AI Risk Management Framework operationalises the AI Policy and Strategy requirements through AI-specific governance and risk controls.

In view of the foregoing, the Board will undertake the following responsibilities:

- b) Establish and approve the institution's Data Governance Strategy which outlines the institution's approach to managing data.
- c) Establish and approve the institution's Data Governance Policy to outline specific mandatory requirements and procedures on the institution's management of data. The Data Governance Policy should, at a minimum, contain the provisions set out in **Annex I**. The policy should be reviewed periodically in accordance with an institution's corporate governance framework.
- d) Establish and approve the institution's data governance framework to cover the institution's approach to data, outline data used for AI purposes, and address AI-specific considerations. An effective data governance framework addresses the following AI considerations:
 - Alignment with the institution's risk appetite and strategy.
 - Clear accountability in different scenarios, including where the financial institution uses its own data, public data, and/or data from third-parties.
 - Basic data literacy for all staff and additional, targeted training for staff working with data.
 - Resources needed for AI data processing, including computation and storage.
 - Procedures for the classification and labelling of data, including metadata.
 - Guidelines for processing unconventional data, and data in different formats.
 - Data security including controls for authorised access and data recovery, and confidential and personal data (including privacy enhancing techniques).
 - An adaptable but consistent approach for assessing data quality and performance.
- e) Establish and approve the institution's AI strategy to support the institution's adoption of AI by providing directions on how the institution will adopt and derive value from AI.
- f) Establish and approve the institution's AI Policy, which establishes the mandatory requirements for responsible use of AI. The AI policy should, at a minimum, contain the provisions set out in **Annex II**. The policy should be reviewed periodically in accordance with an institution's corporate governance framework.
- g) Establish and approve the institution's AI Risk Management Framework to operationalize the AI Policy and Strategy requirements through AI-specific

governance and risk controls. The AI risk management framework should define the institution's AI risk tolerance and risk appetite and ensure they align with the institution's strategic objectives.

- h) Determine the business objectives of using an AI system, including the use cases and justification for using AI.
- i) Establish ethical principles for the development and use of AI that are specific and applicable to the institution.
- j) Determine the permissible and prohibited use of AI in the institution, outlining activities where AI may or may not be used.
- k) Ensure that the use of AI aligns with the vision, mission and strategic goals of the institution.
- l) Establish a Data Governance Committee to implement the institution's data governance strategy, policy, and framework. The committee should comprise representatives from senior management, the Data Protection Officer, the ICT function, legal function, and major business units. The committee should report the effectiveness of the institution's data governance strategy, policy, and framework to the board of directors and senior management periodically.
- m) Establish an AI Governance Committee to implement AI initiatives. The committee should comprise representatives from senior management, the ICT function, legal function, and major business units. The committee should report to the board of directors and senior management periodically on:
 - The adoption of AI in the institution.
 - The effectiveness of the institution's AI strategy and policy.
 - The AI budget and actual expenditure.

The Data and AI Governance Committees may be combined or separate, commensurate with the institution's size, complexity, and risk profile.

- n) Establish a Model Risk Committee to identify, assess, control, manage, report and remediate model risks through the AI life cycle. The committee shall be independent of the functions responsible for the development, implementation and operation of models.

The committee should comprise representatives from senior management, the risk function, and business units. The committee should report the effectiveness of the institution's model risk management to the board of directors and senior management periodically.

The Model Risk Committee may coordinate with the Data Governance Committee and AI Governance Committee on matters relating to data used in ML models and AI systems. However, the Data Governance Committee and AI Governance Committee

shall not perform the independent validation or approval functions assigned to the Model Risk Committee.

- o) Monitor the management's implementation of the data governance and AI strategies, policies, and frameworks.
- p) Ensure the institution is trained on ethical and responsible adoption of AI, AI risks, and risk mitigation, including at the board level.
- q) Allocate adequate resources, expertise, and systems for implementation of the data governance and AI strategies, policies, and frameworks.
- r) Maintain transparent communication and engagement with shareholders and other stakeholders on the uses and governance of AI in the institution.
- s) Review on a regular basis the implementation of the institution's data governance and AI strategies, policies, and frameworks.
- t) Ensure independent review and audit for compliance with set policies and frameworks at least once annually.

4.1.2 Role of Senior Management

Senior management should implement the data governance and AI strategies, policies, and frameworks. The key responsibilities of senior management are outlined below.

- a) Implement the institution's Data Governance Strategy, Data Governance Policy, and Data Governance Framework.
- b) Implement the institution's AI Strategy, AI Policy, and AI Risk Management Framework.
- c) Define and periodically review AI risk ownership and management accountability, assigning clear responsibilities to relevant stakeholders.
- d) Facilitate regular communication of the data governance and AI strategies, policies, and frameworks to all relevant personnel, including internal staff at all levels and, where appropriate, external stakeholders such as third-party technology service providers and business partners.
- e) Coordinate capacity-building initiatives and facilitate training for staff members on the data governance and AI strategies, policies, and frameworks.
- f) Ensure third-party service providers who provide or rely on the institution's AI systems are trained on the institution's expectations, Data Governance Policy, AI Risk Management Framework, and AI Policy.
- g) Monitor data quality, AI risks and report on AI risk management to the board.
- h) Provide regular reports to the board on the institution's adoption of AI, implementation of the Data Governance Strategy, Data Governance Policy, Data Governance Framework, AI Strategy, AI Policy, and AI Risk Management Framework.

4.2 Role of Risk Management Function

Institutions should integrate the AI risk management in their enterprise-wide risk-management frameworks. They should identify, monitor and manage the risks caused by adoption of AI to make well-informed decisions on risk management. The role of the risk management function in managing AI risks includes the following: -

- a) Implement the Model Risk Committee to independently monitor AI risks, assess the effectiveness of AI risk management, and report material AI risks and control deficiencies to senior management and the Board Risk Committee.
- b) Continuously review and report to the Board on risks arising from the institution's adoption of AI.
- c) Periodically assess AI risks and exposures and determine whether they fit within the institution's risk tolerance framework.
- d) Monitor current and emerging AI risks and changes to laws and regulations.
- e) Ensure appropriate risk management and monitoring of third-party AI arrangements.

4.3 Independent Audit and Assessment

The review of AI and data governance frameworks requires a collaborative approach that encompasses multiple functions.

4.3.1 Role of Internal Audit

The internal audit function should:

- a) Assess both the design and effectiveness of the established Data Governance Strategy, Data Governance Policy, Data Governance Framework, AI Strategy, AI Policy, and AI Risk Management Framework at least once annually.
- b) Report the findings of the assessments to the board.
- c) Establish a formal process for following up on audit findings, including the timely verification and remediation of material audit findings that may have an impact on the proper execution of any AI-related activities and business lines.

4.3.2 Role of External Auditors

External auditors have the following responsibilities:

- a) Obtain an understanding of the institution's Data Governance Strategy, Data Governance Policy, Data Governance Framework, AI Strategy, AI Policy, and AI Risk Management Framework, and their impact on financial reporting.
- b) Conduct independent risk assessment of the institution's AI activities.

- c) Conduct comprehensive review of the approved Data Governance Strategy, Data Governance Policy, Data Governance Framework, AI Strategy, AI Policy, and AI Risk Management Framework.
- d) Report annually to the board and CBK on the findings of the AI audits.

4.4 Principles of Ethical and Responsible use of Artificial Intelligence

Institutions' adoption of AI must be underpinned by these guiding principles:

4.4.1 Customer-centricity

Institutions should carefully consider the use cases of AI as well as their benefits and risks, prior to adoption of AI. In this regard, human-centred AI and impact of AI on consumers should be prioritized.

4.4.2 Ethics

This principle requires that any products or services that use AI technologies are reliable and introduced in an ethical manner. The use of AI must in no way compromise with standards set in the banking sector. Introduction of AI technologies in institutions must be done in a manner that respects other players and the customers in the financial sector and in compliance with applicable laws and regulations.

4.4.3 Fairness and Responsibility

Institutions are fully responsible for the outcomes of their adoption of AI. Accordingly, institutions should implement controls to detect and mitigate bias and to ensure that AI-assisted decisions remain subject to appropriate human oversight.

4.4.4 Transparency and Explainability

Customers and key stakeholders must be informed when and how AI technologies are applied in daily operations. Open disclosure and transparency in the use of AI-generated content, data used for AI, and AI-reliant services are essential.

4.4.5 Privacy and Security

Institutions must uphold data privacy and confidentiality, ensuring that the data used to train AI models is treated in accordance with the Data Privacy Act. Institutions must implement adequate cybersecurity measures to ensure the safety and robustness of AI systems and models and the data they use.

4.4.6 Continuous Monitoring

Institutions must establish standards for continuous monitoring and evaluation of AI systems to uphold ethical, legal, and regulatory standards.

4.4.7 Learning and Development

Institutions should commit to continuous learning and development of AI systems through adaptive training, feedback loops, user education, and regular compliance auditing to remain aligned with ethical, legal, and regulatory standards. In pursuit of this principle, institutions must keep abreast of technological and regulatory developments related to AI.

4.5 Data Governance

High-quality data is fundamental to the reliability and effectiveness of AI systems. Institutions are responsible for the quality and representativeness of the data used to train and operate AI systems and models. They must implement strong data governance policies and controls to identify and address historical biases, data gaps, and non-representative datasets that could lead to discriminatory outputs. The data governance framework comprises policies, procedures, and standards for data management, and should include the following aspects:

- a) Data ownership and stewardship for ultimate accountability for a dataset's compliance and value, and the day-to-day management and operational quality of the data, respectively.
- b) Data sources, ensuring data is legally and ethically obtained.
- c) Where personal or confidential information is used for AI systems, institutions shall apply anonymisation, pseudonymisation, masking, tokenisation or other privacy-enhancing techniques. Institutions shall periodically assess the effectiveness of such techniques and the risk of re-identification.
- d) Institutions may generate or use synthetic data for the development, testing, validation, training or operation of AI systems, provided that appropriate governance, risk management and controls are implemented. Institutions shall ensure that the use of synthetic data does not compromise the confidentiality, integrity or availability of information or adversely affect the performance, outcomes, fairness or reliability of AI systems.
- e) Data quality management, including measures for handling missing, duplicate, or inconsistent data.
- f) Data lineage and traceability to track the flow of data for prompt resolution of data quality issues.

- g) Use of training data, ensuring that the training data is representative of the real-world scenario that the AI application will operate in.
- h) Access controls to ensure data is accessed on a need basis.
- i) Data security measures to protect the AI system from cyber threats, including unauthorised access.
- j) Secure data storage with encryption in transit and at rest.
- k) Data retention in line with regulatory requirements and institution's policies.
- l) Ensuring handling of data is in compliance with the Data Protection Act, 2019.

4.6 AI Risk Management Life Cycle

Institutions shall establish, implement, and maintain an AI risk management process to identify, assess, monitor, manage, report, and mitigate risks arising from AI systems throughout their life cycle.

The AI risk management process shall be commensurate with the institution's size, complexity, and risk profile and shall be integrated into the institution's enterprise risk management framework.

The AI risk management life cycle shall comprise:-

- a) Risk identification;
- b) Risk assessment and classification;
- c) Risk treatment and control;
- d) Risk monitoring;
- e) Risk reporting and escalation; and
- f) Periodic review and continuous improvement.

4.6.1 Risk Identification

Institutions shall identify risks arising from AI systems and their use, including:

- Model risk.
- Data risk.
- Operational risk.
- Cybersecurity risk.
- Third-party risk.
- Compliance and legal risk.
- Market conduct risk.
- Financial crime risk.
- Reputational risk.

- Any other risks that may arise from the development, acquisition, deployment, operation, modification, or retirement of AI systems.

4.6.2 Risk Assessment and Classification

Institutions shall assess the likelihood and potential impact of identified AI risks. They shall determine the materiality, criticality, and risk profile of AI systems. The risk assessment shall take into account the intended use of AI, scale, complexity, and potential consequences. It shall also take into account the data quality, model assumptions, limitations, and dependencies. Institutions shall periodically reassess AI risks and classifications.

4.6.3 Risk Mitigation and Control

Institutions shall establish and implement controls and mitigation measures commensurate with the nature, scale, and complexity of the risks identified. Such controls may include measures relating to human oversight, access management, bias mitigation, explainability, cybersecurity, data quality, change management, business continuity, third-party risk management, incident response, and independent validation and testing, where appropriate.

4.6.4 Risk Monitoring

Institutions shall continuously monitor AI systems and associated risks. This includes changes in performance, model drift, and data quality. Additionally, they shall monitor emerging risks, incidents, changes in the operating environment. Further, they shall monitor compliance with internal policies and applicable laws, and the effectiveness of controls and mitigation measures.

4.6.5 Risk Reporting and Escalation

Institutions shall establish procedures for the timely reporting and escalation of material AI risks, incidents, and control deficiencies. Other material AI risks include breaches of internal policies and applicable laws, significant changes to AI systems, model failures, and any other matters that may have a material impact on the institution. Material AI risks and incidents shall be reported to the appropriate governance bodies and senior management in a timely manner.

4.6.6 Periodic Review and Continuous Improvement

Institutions shall periodically review the effectiveness of its AI risk management processes and controls and implement corrective actions where deficiencies are identified.

Institutions shall incorporate lessons learned from incidents and emerging developments and ensure that the AI risk management framework remains appropriate to their size, complexity, and risk profile.

4.6.7 Documentation and Record Keeping

Institutions shall maintain adequate records and documentation to demonstrate compliance with these Guidelines and support effective oversight, monitoring, review, and audit of AI systems and associated risks.

4.7 AI System Life Cycle

Institutions should establish controls throughout the AI life cycle, including:

a) Planning and Design

Institutions should define the objectives, intended use, risk profile, and human oversight arrangements for AI systems.

b) Development or Acquisition

- Institutions should ensure that AI systems are appropriately designed or acquired from reputable third parties and supported by adequate documentation.

c) Training, Testing, and Validation

Institutions should conduct training, testing, and validation before deployment and periodically thereafter to ensure that AI systems perform as intended. The training, testing and validation should include security testing. This is in order to protect sensitive personal data used in the model training and deployment process. Security testing also aims to prevent intentional data manipulation or contamination, and model hijacking.

Human-in-the-loop approach shall be taken in ML model training, testing, and validation. In this regard, human oversight shall include the ability to review the actions of the ML model or AI system.

d) Deployment and Operation

- Institutions shall seek approval of the Central Bank prior to deployment of AI systems. The application for approval shall be made in writing and be accompanied by the Data Governance and Artificial Intelligence Checklist as specified in **Annex III**.

- Institutions should establish approval processes, user training, and controls to ensure the safe operation of AI systems.
- Financial institutions must conduct bias impact assessments before deploying an AI system.
- Institutions should incorporate a Fairness-by-Design approach by embedding fairness considerations.
- Model designers and developers should use technical tools to measure and enforce fairness metrics appropriate to the specific use case.
- Institutions should mitigate discriminatory outcomes based on protected attributes such as race, gender, ethnicity, religion, nationality, disability, or age.
- Institutions must ensure that AI-enabled services do not inadvertently exclude or disadvantage vulnerable groups, for instance, customers who lack access to smartphones.
- Institutions should ensure that AI systems do not directly or indirectly use sensitive personal data as factors in decision-making.
- Institutions should not use AI systems, personal data, or proxies for data (e.g. using postal code to deduce race or ethnicity) in a manner that results in digital redlining or any other form of unfair discrimination.

e) Monitoring and Review

- Institutions should continuously monitor AI systems for performance deterioration, model drift, bias, security vulnerabilities, and other emerging risks.
- Institutions should conduct periodic fairness and bias audits of AI systems and models, with documentation of results and remedial actions to affected consumers.
- AI systems must be evaluated and monitored to prevent bias and ensure fair treatment, with no discriminatory outcomes based on protected attributes such as race, gender, ethnicity, religion, nationality, disability, or age.

f) Retirement and Decommissioning of AI Systems

- i) Institutions should ensure that obsolete AI systems are retired in a controlled manner and that records are retained in accordance with applicable requirements.
- ii) Institutions shall establish and implement procedures for the orderly retirement and decommissioning of AI systems.
- iii) Before retiring or decommissioning an AI system, institutions shall:
 - Assess and manage the associated operational, legal and regulatory risks.
 - Ensure the continuity of critical services.
 - Securely retain, archive or dispose of data, models and records in accordance with applicable legal and regulatory requirements.

- Revoke access to, and securely remove or disable, the AI system and associated resources.
- iv) Institutions shall maintain records of the retirement or decommissioning of material or high-risk AI systems.

4.8 Model Risk Management

Institutions should incorporate AI model risk within their broader risk management framework. They should maintain an inventory of all AI systems and models in use and implement independent validation and periodic reviews of AI models. Review of AI model risk should be undertaken by the Model Risk Committee and should include the following aspects:

- Model selection, development and training.
- Model bias and fairness baselines.
- Model explainability.
- Data quality assurance.
- Model validation and testing.
- Model performance baselines and metrics.
- Model stress testing.
- Benchmarking against existing benchmarks or industry standards.
- Model deployment and monitoring processes and procedures.
- Feedback loop for improving the model.
- Supply chain model risks for third-parties, fourth parties, and n-th parties.
- Model updates.

4.9 Third-Party AI Risk Management

Institutions must remain accountable for AI systems provided by third parties. Where AI systems are obtained from third parties, institutions should adhere to relevant regulatory requirements, including the requirements of the Guidance Note on Third-Party Technology Service Providers, Prudential Guidelines, and Risk Management Guidelines. Further, institutions should undertake due diligence on such arrangements and consider the following:

- Service dependencies;
- Concentration risk;
- Contractual arrangements;
- Data ownership and portability;
- Cybersecurity;

- Explainability and transparency; and
- Exit strategies.

Institutions should ensure that third-party AI vendors comply with their AI and data governance policies. Additionally, they should consider how they can ensure control over the AI systems parameters and outputs.

4.10 Generative AI

- a) Institutions that are considering the adoption of generative AI should ensure that their AI strategies and policies are updated with the following aspects.
 - i) Acceptable use policies;
 - ii) Confidentiality of customer and proprietary information;
 - iii) Output validation and human review;
 - iv) Hallucination/confabulation risks;
 - v) Intellectual Property considerations;
 - vi) Prompt management; and
 - vii) Employee awareness and training.
- b) Institutions should ensure that material decisions are not based solely on unverified outputs generated by AI systems.
- c) Institutions should establish baseline metrics for factual consistency in the use of generative AI.

4.11 Agentic AI

4.11.1 High-Risk Classification

An agentic AI system that is capable of independently initiating actions, interacting with external systems, executing transactions or materially affecting the institution's operations shall be classified as a high-risk AI system and shall be subject to enhanced governance and independent review.

4.11.2 Use of Agentic AI

- a) Institutions shall not deploy or use agentic AI systems unless they have established appropriate governance, risk management and control measures commensurate with the nature, scale and complexity of the system.

- b) Institutions shall ensure that agentic AI systems:
- i) Operate within clearly defined objectives and authorised parameters.
 - ii) Remain subject to effective human oversight and intervention.
 - iii) Are capable of being monitored, suspended or terminated where necessary.
 - iv) Maintain appropriate records of its activities, actions and decisions.
 - v) Comply with applicable legal, regulatory and internal requirements.
- c) In deploying agentic AI systems, institutions shall ensure human oversight is enabled, including the ability to review the actions of the system, intervene in or override the operation of the system; and suspend or terminate the system where necessary.
- d) Institutions shall ensure that AI agents and agentic AI systems:
- i) Operate within predefined authority limits.
 - ii) Do not modify their objectives or operating parameters without appropriate authorisation.
 - iii) Are protected against unauthorised access or manipulation.
 - iv) Maintain complete audit logs of material actions and decisions.
 - v) Are subject to continuous monitoring.
- e) Where an institution procures or uses an agentic AI system or AI agent provided by a third-party technology service provider, the institution shall ensure that the arrangement complies with this Guidance and that the provider enables the institution to exercise effective oversight, monitoring and control over the system.

4.12 AI Incident Management

Institutions should establish processes for identifying, reporting, investigating, and responding to AI-related incidents, including:

- Model failures;
- Unintended outcomes;
- Bias or discriminatory effects;
- Security breaches;
- Data leakage;
- System outages; and
- Significant performance deterioration.

Institutions should incorporate lessons learned from incidents into their AI governance and risk management frameworks.

4.13 Documentation and Record Keeping

Institutions should maintain adequate records relating to AI systems, including:

- **AI model inventories and technical documentation** - Develop documentation outlining the design of the material AI models and systems. This includes creating a guide that explains how the AI models operate and documenting the system design and architecture that has been used in AI development.
- **Audit logs** - Maintain audit logs and traceability of decisions and outcomes of the AI system.
- **Testing and validation results** - Develop frameworks to monitor model performance and detect model drift, where a model's performance degrades or becomes unreliable over time due to shifts in real-world data. Document and maintain the testing and validation results.
- **Original data sets** – Institutions should keep a record of all original datasets used for training AI models.
- **Approvals** - Maintain a record of all regulatory and institutional approvals on AI activities.
- **Contracts:** - Maintain the contract records, including changes and updates to the contracts.
- **Incidents** - Maintain incident reports as required.
- **Changes and updates** - Maintain documentation on changes and updates to AI systems and models.

4.14 Training and Awareness

Institutions should provide appropriate training and awareness programmes for the Board, senior management, staff, and relevant third parties to promote the ethical and responsible use of AI.

4.15 Consumer Protection and Market Conduct

4.15.1 Disclosure Obligations

- a) Institutions must ensure transparency to customers in their use of AI. Customers should be aware when they are interacting with an AI system and understand how AI-driven decisions affecting them are made. The terms and conditions of AI-related services and products should include information on the use of AI for service delivery.
- b) Institutions must clearly disclose to customers when an AI system is overseeing a primary interaction. This disclosure should be made at the initial point of interaction in a simple and unambiguous manner.

- c) Disclosures must be provided in plain language that is understandable to the average customer, avoiding excessive technical jargon.
- d) Institutions should ensure that customers are informed of products or services that utilize AI, the associated risks, and limitations of the technology prior to providing the service initially.
- e) Each update of an AI system will be treated as a latest version requiring customer notification.
- f) Institutions should collect customer consent to accept the risks associated with the use of AI prior to providing the service.
- g) Consumers shall be informed about the categories of data being collected, processed, and used in AI systems, as well as their rights regarding consent and withdrawal.
- h) Institutions shall, upon request, provide customers with a clear explanation of the data, variables, and factors that inform the decision-making processes of its AI systems.
- i) Institutions should provide a visible and accessible feedback channel for questions or comments.

4.15.2 Human Review for Critical Decisions

Customers must have the right to request and obtain human intervention in the review of significant, adverse decisions made by AI systems, to challenge the decision, and to provide supporting data.

Institutions must provide consumers with information on their right to request human review of critical decisions made or supported by AI. Institutions must establish clear internal processes through which customers can contest AI-driven outcomes and request reconsideration by qualified human staff.

i) Human Review Process

- a) The human review must be conducted by an individual with the appropriate authority, training, and competence to evaluate the AI's decision and the customer's specific case.
- b) The reviewer must have access to all data points used by the AI, the logic behind the decision, to the extent possible, and any additional information provided by the customer.
- c) Institutions must establish and disclose expected timeframes for resolution.

ii) Outcome of Review

- a) Institutions should ensure that decisions, particularly those that negatively affect consumers, can be explained in a meaningful way, highlighting the main factors that influenced the AI system's output.
- b) Following the review, institutions must communicate the outcome to the customer, including the reasoning behind the human reviewer's decision. If the original decision is overturned, institutions must take all necessary steps to rectify the situation promptly.
- c) Institutions ensure that staff reviewing AI-driven decisions exercise independent judgment and are not overly reliant on the AI recommendation.

4.15.3 Complaints Redress Mechanisms

Institutions must establish effective complaints redress mechanisms specifically designed to handle complaints related to AI systems. This includes:

- a) Ensuring that customers can submit complaints regarding AI-related decisions through multiple channels (physical branches, call centres, online portals, mobile applications).
- b) Establishing a clear escalation path for complaints.
- c) Investigate and resolve complaints promptly within prescribed timelines.
- d) Maintain a register of AI-related complaints, their resolution, and remedial actions taken to address recurring issues.
- e) Analyse AI complaints regularly to identify systemic issues, biases, or performance failures in AI systems and models, triggering model retraining or decommissioning where necessary.

PART V: REPORTING

- (1) Institutions shall provide the Central Bank with a register of their AI models, systems, and services in the format set out in **Annex IV (Annual)**. The register shall be submitted immediately upon this Guidance Note taking effect, and thereafter by the 5th day after the end of every financial year.
- (2) Institutions should notify the Central Bank of Kenya within 24 hours of any AI incident that materially affects service availability, confidentiality, integrity, or incident(s) that could have a significant and adverse impact on the institution's ability to provide adequate services to its customers, its reputation or financial condition in the format set out in **Annex V (Immediate)** to this Guideline.

- (3) Institutions should submit a report as set out in **Annex VI**, within 24 hours of resolution of a critical incident, indicating the cause, origin (internal or third party), remedial actions, lessons learned and supporting documentation (investigation reports or technical logs).
- (4) On a quarterly basis, by the 5th day after the end of every quarter, institutions shall provide the Central Bank with a report in the format set out in **Annex VII (Quarterly)** to this Guideline, concerning its occurrence and handling of AI incidents via the email address: fin@centralbank.go.ke.

ANNEX I

High-Level Contents of a Data Governance Policy

An institution's Data Governance Policy should, at a minimum, include the following: -

1. Purpose and Scope
2. Data Governance Principles
 - Data as an organisational asset.
 - Data ownership and accountability.
 - Appropriate use of data.
 - Data quality.
 - Security and confidentiality.
 - Availability and accessibility.
 - Data privacy.
 - Transparency and traceability.
 - Data minimisation.
 - Retention and disposal.
 - Appropriate use and sharing.
3. Governance Structure
 - Role of the Board.
 - Role of Senior Management.
 - Role of Risk Management.
 - Role of Internal Audit.
 - Data Governance Committee.
 - Chief Data Officer/Data Governance Lead.
 - Data Owners: Accountable for specific data domains.
 - Data Stewards: Manage quality, definitions, metadata and day-to-day controls.
 - Data Custodians/IT: Technical storage, access, security and availability.
 - Data Users: Comply with approved access and usage requirements.
4. Data Classification
 - Classification requirements and corresponding handling controls.
 - Public
 - Internal
 - Confidential
 - Restricted
5. Data Ownership and Stewardship
 - Every critical data domain should have a designated owner and steward.
 - Responsibilities should include quality, access, classification, retention and appropriate use.
6. Data Quality Management

- Establish standards/ mandatory requirements for accuracy, completeness, consistency, validity, uniqueness and timeliness.
 - Define processes for identifying, correcting and reporting data-quality issues.
7. Data Access and Usage
- Access authorisation/approval, least privilege, need-to-know and appropriate-use requirements.
 - Periodic reviews.
 - Logging and monitoring of sensitive-data access.
8. Data Privacy and Protection
- Compliance with Data Protection Act, 2019.
 - Lawful collection and processing, privacy, confidentiality and protection of personal/sensitive data.
 - Purpose limitation and data minimisation.
 - Management of data-subject rights and privacy risks.
9. Data Lifecycle Management
- Requirements covering collection, creation, storage, use, sharing, archiving, retention and secure disposal.
11. Metadata and Data Catalogue
- Maintain definitions of critical data elements.
 - Document data lineage, sources, owners, systems and permissible uses.
12. Data Sharing
- Requirements for internal and external data sharing.
 - Due diligence and contractual controls.
 - Cross-border transfer requirements where applicable.
13. Third-Party and Outsourced Data
- Governance requirements where data is processed, stored or managed by third parties.
14. Data Security
- Protection against unauthorised access, alteration, loss or destruction.
15. Data Governance for AI
- Data used to develop, train, validate and operate AI systems should meet defined quality, provenance, privacy, security and bias-management requirements.
 - AI data sources should be documented and appropriately authorised.
 - Data lineage should be maintained for material AI systems.
16. Data Risk Management
- Identify and assess data risks.
 - Maintain a data-risk register.
 - Establish controls, risk indicators and escalation procedures.
17. Records Management and Retention
- Define retention periods by data category.
 - Ensure legal/regulatory holds are respected.

- Securely dispose of data when retention periods expire.
18. Regulatory and Legal Compliance
- Compliance with applicable data protection, banking, records-management and other regulatory requirements.
19. Monitoring and Reporting
- Compliance monitoring, reporting, assurance and management of data-governance issues, including:
 - Data-quality KPIs, policy compliance, access violations.
 - Data incidents.
 - Critical-data issues.
 - Reporting, escalation and remediation requirements.
20. Exceptions
- Process for approving, documenting and reviewing policy exceptions.
21. Training and Awareness
- Mandatory data-governance and data-protection training.
 - Role-specific training for data owners, stewards and custodians.
22. Consequences of Policy Breaches/Non-Compliance
- Consequences and corrective actions for breaches of the policy.
23. Policy Review and Update

ANNEX II

High-Level Contents of an Artificial Intelligence Policy

An institution's Artificial Intelligence (AI) Policy should, at a minimum, include the following: -

1. Purpose and scope.
2. Ethical Use of AI.
 - Acceptable Use of AI.
 - Ethical Considerations.
3. Ethical Principles and Guidelines.
 - Transparency.
 - Fairness.
 - Accountability.
 - Privacy.
4. AI Impact Assessment.
5. Legal and Regulatory Compliance.
 - Compliance with all relevant local, national, and international laws and regulations.
 - Data Protection Act and Regulations.
6. Governance Structure.
 - AI Governance Committee.
 - Data Governance Committee.
 - Roles and Responsibilities.
7. Risk Management.
 - Risk Identification, Assessment, Mitigation and Monitoring.
 - Incident Response.
8. Data Governance.
 - Data Quality.
 - Data Privacy.
 - Data Security.
 - Data Ownership.
9. Bias and Fairness.
 - Bias Detection.
 - Fairness Audits.
10. Transparency and Explainability. How the model arrives at its decisions and is this level of transparency sufficient for the use case?
 - Model Transparency.
 - Documentation.
11. Accountability and Responsibility.
 - Accountability Framework.
 - Reporting Mechanisms.

12. AI Development and Deployment.

- AI development lifecycle: Problem Definition and Scoping, Data Acquisition and Preparation, Model Development and Training, Model Evaluation and Refinement, Deployment, Monitoring and Maintenance.

13. Continuous Monitoring and Evaluation.

- Performance Monitoring.
- Periodic Reviews, Retraining and Updates.

14. Human-AI Interaction.

- User-friendliness.
- AI explainability.
- Human oversight.

15. Training and Education.

- Employee Training.
- Awareness Programs.

16. Collaboration and Engagement.

- Stakeholder Engagement.
- Industry Collaboration.
- Feedback mechanisms.

17. Review and Update of the AI Policy.

ANNEX III
Data Governance and Artificial Intelligence Checklist

NO.	QUESTION	YES	NO	DESCRIPTION
1.	Name of the AI-based application, if applicable.			
A. DATA GOVERNANCE AND RISK MANAGEMENT				
2.	Does the institution have a Data Strategy, Data Policy, and Data Governance Framework? <i>If yes, attach.</i>			
3.	Data Governance Committee: Does the institution have a Data Governance Committee to implement the institution's data governance strategy, policy, and framework and enforce data governance practices? If yes, provide details on the composition of the committee and the terms of reference.			
4.	Data Sources: What are the data sources for use in the AI-based application? Are they legally and ethically obtained?			
5.	Data Quality: How is data quality ensured? Are there measures for handling missing, duplicate, or inconsistent data?			
6.	Training Data: Is the training data representative of the real-world scenario that the AI application will operate in?			
7.	Data Security: What security measures are in place to protect the AI system from cyber threats, including unauthorised access?			
8.	Secure Data Storage: What measures are in place to ensure data security? How is data encrypted during storage and transmission?			

NO.	QUESTION	YES	NO	DESCRIPTION
9.	Security Testing: Has the App undergone security testing? What security measures are in place to protect sensitive data used in the model training and deployment process? What measures are in place to prevent intentional data manipulation or contamination?			
10.	Regulatory Compliance: Does the institution ensure their handling of data is in compliance with the Kenya Data Protection Act, 2019?			
B. AI GOVERNANCE AND RISK MANAGEMENT				
11.	Does the institution have an AI Strategy, AI Policy and AI Risk Management Framework? <i>If yes, attach.</i>			
12.	AI Governance Committee: Does the institution have an AI Governance Committee to oversee AI initiatives and ensure compliance with the institution's AI policy? If yes, provide details on the composition of the committee and the terms of reference.			
13.	Ethical Considerations			
3.1	Transparency			
3.1.1	What are the proposed uses of AI by the institution?			
3.1.2	Are customers informed about the use of AI in the application, and is their consent obtained? <i>Attach consent form and terms and conditions.</i>			
3.1.3	Is there clear information provided to customers about how AI is used?			

NO.	QUESTION	YES	NO	DESCRIPTION
3.1.4	Are there clear instructions that avoid ambiguity, and mechanisms for customers to give feedback on the AI?			
3.1.5	How transparent is the AI system in terms of its capabilities and limitations?			
3.2	Fairness			
3.2.1	Are there any biases in the data that could impact the model's performance?			
3.2.2	Does the model treat all users fairly, regardless of their background?			
3.2.3	How are potential bias/discriminatory outcomes handled?			
3.3	Accountability			
3.3.1	Who is accountable and responsible for the decisions, actions, and outcomes made by the AI system?			
3.3.2	Are there mechanisms in place to address errors or harms caused by the AI?			
3.3.3	Has an impact assessment been conducted to understand the potential impact of the AI system on customers, business, and society?			
3.4	Privacy			
3.4.1	Does the institution comply with the Kenya Data Protection Act, 2019 and other relevant data privacy laws and regulations?			
3.4.2	How is sensitive personal data handled?			
3.5	Documentation and Communication			
3.5.1	Documentation: Is there comprehensive documentation covering all aspects of the AI application's life cycle, including development, testing, and deployment?			
3.5.2	Communication: Does the institution have policies on communication to key stakeholders about the AI system's functionality, updates, and issues?			

NO.	QUESTION	YES	NO	DESCRIPTION
14.	Training and Education: Are staff educated on how to interact with the AI system and understand its outputs?			
	C. MODEL RISK MANAGEMENT			
15.	Model Risk Committee Does the institution have a Model Risk Committee? If yes, provide details on the composition of the committee and the terms of reference.			
16.	Model Development and Training			
14.1	Model Selection: What criteria are used to select the machine learning models?			
14.2	Bias and Fairness: How is bias detected and mitigated in the training data and model?			
14.3	Explainability: How explainable is the model's decision-making process? Can the decisions be understood and interpreted by humans?			
14.4	Data: Is the training data representative of the real-world scenario?			
17.	Model Bias			
15.1	Has the model been evaluated for bias in terms of location, gender, and age, among others?			
15.2	What steps have been taken to mitigate bias?			
18.	Model Validation and Testing			
16.1	Validation:			
16.1.1	How is the model validated, and are there separate datasets for training, validation, and testing?			
16.1.2	Has the model been tested on real-world data? Is the data diverse enough to prevent bias?			
16.2	Performance Metrics:			

NO.	QUESTION	YES	NO	DESCRIPTION
16.2.1	What performance metrics are used to evaluate the model? Are they appropriate for the institution's AI use case?			
16.2.2	What is the prediction accuracy for ML model?			
16.2.3	How does the model perform on different subsets of the data?			
16.3	Stress Testing: Has the model been stress-tested under various scenarios to ensure robustness? How does the model handle adversarial attacks or malicious inputs designed to disrupt its performance? Can the model adapt to changing data distributions over time?			
16.4	Benchmarking: How does the model performance compare to existing benchmarks or industry standards?			
19.	Model Deployment and Monitoring			
17.1	Deployment Process: What is the process for deploying the model into production? Are there safeguards to prevent untested models from being deployed?			
17.2	Monitoring: How is the model's performance monitored post-deployment? Are there automated systems in place to detect performance degradation?			
17.3	Feedback Loop: Is there a mechanism for collecting user feedback and using it to improve the model?			
17.4	Model Updates: How are model updates managed? Is there a process for rolling back to a previous version if necessary?			
20.	Monitoring and Evaluation			
18.1	Are there plans for continuous monitoring and evaluation of the model's performance and impact?			

NO.	QUESTION	YES	NO	DESCRIPTION
18.2	Is there a mechanism for collecting user feedback and using it to improve the model?			
21.	Third Parties			
19.1	Does the institution use outsourced AI vendors, or third-party tools or libraries? How is their security and compliance ensured?			
19.2	How does the institution ensure that third-party AI vendors comply with data protection laws and regulations?			
19.3	What control measures does the institution have over the AI systems parameters and outputs, for instance, incorrect output?			
22.	Decommissioning Plan			
20.1	Is there a decommissioning plan to ensure critical AI services can continue operating during decommissioning of AI systems? If yes, provide details.			

ANNEX IV
Artificial Intelligence Deployment Register (Annual)

Submit this report on the 5th day after the end of every financial year to the Bank Supervision Department at fin@centralbank.go.ke

[Insert Name of person reporting]

[Quarter]: Year.....

No.	Name of Artificial Intelligence (AI) Model/ System Deployed	Date of CBK Approval	AI Service Provider (Internally developed, acquired, third-party)	AI Services	Critical/ Non-Critical Classification*	Jurisdiction where Service is Performed, where applicable	Jurisdiction where the data is stored or hosted	Last Date of Model Testing	Last Date of Cybersecurity Testing
1.									
2.									
3.									
4.									
5.									

Signed for and on behalf of

By the duly authorized signatories:

Name.....

Designation.....

Contact email address.....

Contact phone number.....

Signature.....

Name.....

Designation.....

Contact email address.....

Contact phone number.....

Signature.....

ANNEX V
Artificial Intelligence Incident Record (Immediate)

Artificial Intelligence Incident Record (*Immediate*)

[Insert Name of reporting financial institution]

[Insert Date and Time of reporting]: Date..... Time.....

Date of Incident	Time of Incident	Critical Artificial Intelligence (AI) Service	Incident Status (Open, Resolved or Closed)	Nature of Incident (Chronological order of events)	Impact Assessment	Actions taken by the time of reporting

Submit the critical AI incident report within 24 hours after a material incident(s) to the Bank Supervision Department at fin@centralbank.go.ke

Authorised Signatories

Signed for and on behalf of

By the duly authorized signatories:

Name.....

Designation.....

Contact email address.....

Contact phone number.....

Signature.....

Name.....

Designation.....

Contact email address.....

Contact phone number.....

Signature.....

ANNEX VI

Artificial Intelligence Incident Record (Final)

Artificial Intelligence Incident Record (*Upon Resolution*)

[Insert Name of reporting financial institution]

[Insert Date and Time of reporting]: Date..... Time.....

Final Incident Report	
Date and time incident occurred:	
Date and time of resolution:	
Date and time of closure:	
Incident discovery method (how or via which channel was the incident discovered)	
Changes since the AI Incident Record (<i>Immediate</i>) (detailed chronological event, stakeholders notified):	
Impact assessment (financial loss amount, data loss, assessment on reputational impact based on customer complaints, description of systems affected as well as associated services):	
Incident description (Location, purpose of the system, name of service provider affected where applicable, affected applications /databases/ networks / storage / servers, etc.	
Incident closure (Indicate the root cause of the incident):	
Lessons and remediation:	

Submit the critical AI incident report within 24 hours after resolution of a critical AI incident to the Bank Supervision Department at fin@centralbank.go.ke

Authorised Signatories

Signed for and on behalf of

By the duly authorized signatories:

Name.....

Designation.....

Contact email address.....

Contact phone number.....

Signature.....

Name.....

Designation.....

Contact email address.....

Contact phone number.....

Signature.....

ANNEX VII
Artificial Intelligence Incident Record (Quarterly)

[Insert Name of reporting financial institution]

[Quarter]..... [Year]

No.	Date of Incident	Time of Incident	Critical Artificial Intelligence (AI) Service	Nature of Incident	Action Taken	Time of Resolution	Impact Assessment	Action Taken to Mitigate Future Incidents
1.								
2.								
3.								
4.								
5.								

Submit this report on the 5th day after the end of every quarter to the Bank Supervision Department at fin@centralbank.go.ke

Signed for and on behalf of

By the duly authorized signatories:

Name.....
 Designation.....
 Contact email address.....
 Contact phone number.....
 Signature.....

Name.....
 Designation.....
 Contact email address.....
 Contact phone number.....
 Signature.....

REFERENCES

1. Artificial Intelligence Act. (2024). *Brazil AI Act*.
<https://artificialintelligenceact.com/brazil-ai-act/>
2. Bank for International Settlements. (2024, December 12). *Regulating AI in the financial sector: Recent developments and main challenges* (FSI Insights on policy implementation No. 63). <https://www.bis.org/fsi/publ/insights63.pdf>
3. Bank for International Settlements. (2026, March 26). *In data we trust? Emerging policy and supervisory approaches to AI data use in financial services* (FSI Insights on policy implementation No. 73). <https://www.bis.org/fsi/publ/insights73.pdf>
4. Central Bank of Kenya. (2025, July 3). *Survey on artificial intelligence in the banking sector*.
https://www.centralbank.go.ke/uploads/banking_sector_reports/595566510_Survey%20on%20Artificial%20Intelligence%20in%20the%20Banking%20Sector.pdf
5. European Commission. (2025, February 4). *Commission publishes the guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act*.
<https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>
6. European Parliament. (2025, February 19). *EU AI Act: First regulation on artificial intelligence*. <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>
7. European Parliament and Council of the European Union. (2022, December 14). *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. *Official Journal of the European Union*. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554>
8. Financial Conduct Authority. (2024, April 22). *AI update*.
<https://www.fca.org.uk/publication/corporate/ai-update.pdf>
9. Financial Stability Board. (2024, November 14). *The financial stability implications of artificial intelligence*. <https://www.fsb.org/uploads/P14112024.pdf>
10. Financial Stability Board (FSB). (2026, June 10). *Sound Practices for Responsible Adoption of Artificial Intelligence (AI): Consultation Report*.
<https://www.fsb.org/2026/06/sound-practices-for-responsible-adoption-of-artificial-intelligence-ai-consultation-report/>
11. Gilliard, C. (2019, November 21). *Prepared testimony and statement for the record* [Testimony before the U.S. House Committee on Financial Services, Task Force on Financial Technology, hearing on “Banking on Your Data: The Role of Big Data in Financial Services”].
<https://www.congress.gov/116/meeting/house/110251/witnesses/HHRG-116-BA00-Wstate-GilliardC-20191121.pdf>

12. IBM. (n.d.). *Maximizing compliance: Integrating gen AI into the financial regulatory framework*. <https://www.ibm.com/think/insights/maximizing-compliance-integrating-gen-ai-into-the-financial-regulatory-framework>
13. Irving Fisher Committee on Central Bank Statistics. (2026). *Generative artificial intelligence in central banking* (IFC Bulletin No. 67). Bank for International Settlements. https://www.bis.org/ifc/publ/ifcb67_01_rh.pdf
14. KPMG AG Wirtschaftsprüfungsgesellschaft. (2016). *Model risk management: A sound practice for meeting current challenges*. KPMG. <https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/KPMGModelRiskManagement2016.pdf>
15. Ministry of Information, Communications and the Digital Economy. (2025). *Kenya AI strategy 2025–2030*. Government of Kenya. <https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf>
16. Monetary Authority of Singapore. (2018). *FEAT principles: Fairness, ethics, accountability and transparency*. <https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/feat>
17. Monetary Authority of Singapore. (2025). *Consultation paper on guidelines on artificial intelligence risk management*. <https://www.mas.gov.sg/publications/consultations/2025/consultation-paper-on-guidelines-on-artificial-intelligence-risk-management>
18. National Institute of Standards and Technology. (2024, July). *Artificial intelligence risk management framework: Generative artificial intelligence profile* (NIST AI 600-1). <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>
19. Norton Rose Fulbright. (2025, July 2). *AI regulation in financial services: FCA developments and emerging enforcement risks*. <https://www.regulationtomorrow.com/2025/07/ai-regulation-in-financial-services-fca-developments-and-emerging-enforcement-risks/>
20. OECD AI Policy Observatory. (n.d.). *OECD AI principles*. <https://oecd.ai/en/ai-principles>
21. Organisation for Economic Co-operation and Development. (2024, September 4). *Regulatory approaches to artificial intelligence in finance*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/09/regulatory-approaches-to-artificial-intelligence-in-finance_43d082c3/f1498c02-en.pdf
22. Senado Federal. (2023, May 3). *Projeto de Lei nº 2338, de 2023: Dispõe sobre o uso da Inteligência Artificial*. <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>
23. U.S. Department of the Treasury. (2024, December). *Artificial intelligence in financial services: Report on the uses, opportunities, and risks of artificial intelligence in the financial services sector*. <https://home.treasury.gov/system/files/136/Artificial-Intelligence-in-Financial-Services.pdf>
24. White & Case LLP. (2025, June 6). *AI watch: Global regulatory tracker - Brazil*. <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-brazil>