AI GOVERNANCE POLICY

For Banks and Financial Institutions in Ghana

The policy is informed by LAWSMORE's SAFE-AI Principles, which encourage the use of AI systems that are Secure, Accountable, Fair, Explainable, Africa-Centered, and Impact-Driven. These principles guide every decision the Bank makes regarding the design, procurement, deployment, and monitoring of AI systems.

LAWSMORE
11/22/2025

Contents

EXECUTIVE SUMMARY

Artificial Intelligence is becoming an essential part of modern financial services. Banks are already using AI to strengthen fraud monitoring, improve customer service, speed up credit assessment, and support regulatory compliance. While these opportunities are significant, the risks are equally important. Poorly governed AI systems can produce inaccurate decisions, expose the Bank to data protection breaches, create fairness concerns, weaken cybersecurity, and diminish public trust.

This policy provides a clear and organised framework for the responsible use of AI within the Bank. It explains the regulatory obligations the Bank must meet, establishes principles for ethical and transparent AI use, outlines how risks should be assessed and mitigated, and assigns responsibilities across governance structures. By following this policy, the Bank commits to adopting AI in a manner that protects customers, strengthens institutional resilience, and enhances the reputation of the financial sector in Ghana.

The policy is informed by LAWSMORE's SAFE-AI Principles, which encourage the use of AI systems that are Secure, Accountable, Fair, Explainable, Africa-Centered, and Impact-Driven. These principles guide every decision the Bank makes regarding the design, procurement, deployment, and monitoring of AI systems.

1. PURPOSE, SCOPE AND APPLICABILITY

1.1 Purpose

This policy aims to provide a consistent and reliable approach for managing the risks and opportunities associated with Artificial Intelligence. It serves five main purposes. First, it establishes the minimum governance standards required before an AI system can be introduced into the Bank. Second, it ensures that all AI use remains compliant with the laws of Ghana, the directives of the Bank of Ghana, and recognised global standards. Third, it outlines the safeguards needed to protect customer information and maintain the confidentiality, integrity, and availability of data. Fourth, it promotes the ethical and transparent use of AI, particularly when automated systems influence decisions affecting customers. Finally, it supports the Bank's broader digital transformation journey by ensuring that innovation is balanced with accountability.

1.2 Scope

This policy applies to all forms of Artificial Intelligence used by the Bank. This includes predictive models, machine learning systems, automated decision-making tools, natural language systems, generative AI platforms, robotic process automation, and all other technologies that perform functions which normally require human intelligence.

It covers internal AI systems developed by the Bank, third-party AI solutions purchased from vendors, cloud-based tools, and any data used to train or support these systems. The policy also applies to experimental or pilot AI projects, even if they have not yet been deployed fully.

1.3 Applicability

This policy applies to every employee of the Bank. It also covers contractors, interns, external consultants, and any third-party vendors who design, implement, or manage AI systems on behalf of the Bank.

When there is any conflict between this policy and another internal policy, the stricter requirement should be applied. Where laws or regulations impose higher standards than this policy, the Bank will comply with the external requirement.

2. INTRODUCTION TO AI FOR FINANCIAL SERVICES

2.1 Understanding Artificial Intelligence in Banking

Artificial Intelligence refers to technological systems that can learn, analyse, predict, or make decisions using data. In the banking context, AI is often embedded in tools that detect fraudulent transactions, assess loan applicants, classify risks, automate repetitive processes, and analyse large volumes of customer information.

Some common examples in the financial sector include systems that identify unusual patterns in transactions, algorithms that generate risk alerts, chatbots that guide customers through basic banking interactions, tools that verify identity through facial or document recognition, and analytical models that help the Bank understand customer behaviour.

2.2 Why AI Is Important to the Bank

AI has the potential to significantly improve how the Bank operates. It can make processes faster and more efficient, reduce human error, strengthen fraud detection, and provide customers with faster and more personalised services. It can also support compliance monitoring by helping the Bank identify irregular patterns or potential regulatory breaches.

However, these advantages come with important risks. AI systems may produce inaccurate or biased results if they are not properly designed or monitored. They may expose the Bank to cybersecurity threats if external tools are used without safeguards. They may process customer data in ways that violate the Data Protection Act. The Bank may also face reputational harm if AI tools give customers inaccurate information or make unfair decisions.

For this reason, the Bank must treat AI adoption with a high level of discipline.

2.3 Connection to Bank of Ghana Priorities

Artificial Intelligence directly touches the priority areas of the Bank of Ghana. The central bank places strong emphasis on cybersecurity, operational risk management, outsourcing controls, and customer protection. AI systems operate within all these areas.

The Bank must therefore ensure that any AI tool deployed is secure, well-documented, tested, traceable, and managed throughout its life cycle. AI adoption is not simply a technology decision; it is a regulated activity that requires oversight and accountability.

3. REGULATORY, LEGAL AND STANDARDS FRAMEWORK

3.1 The Data Protection Act of Ghana

AI use within the Bank must comply with the Data Protection Act (Act 843). This requires the Bank to ensure that all personal data processed by AI systems is collected lawfully, used only for legitimate purposes, stored securely, and protected from unauthorised access.

The Bank must limit the amount of data fed into AI systems, especially when using external or cloud-based tools. Customers have rights under the Act, including the right to be informed, the right to access their data, and the right to object to certain forms of automated processing. The Bank must ensure that its AI systems do not undermine these rights.

3.2 Bank of Ghana Regulations

Several directives from the Bank of Ghana directly affect the use of AI. These include:

- The Cyber and Information Security Directive
- The ICT Risk Management Guidelines
- The Outsourcing and Third-Party Risk Guidelines
- The Operational Risk Management Framework

Each of these frameworks requires the Bank to put controls in place to protect systems, manage third-party risks, maintain strong internal controls, and ensure transparent reporting of incidents. Any AI system introduced into the Bank must meet these requirements.

3.3 International Standards and Global Benchmarks

Although Ghana has not yet issued a dedicated AI law, several international frameworks provide guidance that is useful for the Bank. These include the European Union's AI Act, the OECD Principles on Artificial Intelligence, the ISO standards on AI management and risk, the African Union's emerging AI strategy, and GIZ Ghana AI Practitioners Guide.

The Bank will align its practices with these standards where they support responsible AI use. When inconsistencies arise, the Bank will prioritise compliance with the laws of Ghana and directives of the Bank of Ghana.

4. LAWSMORE SAFE-AI PRINCIPLES

The Bank adopts the SAFE-AI Principles developed under the LAWSMORE framework. These principles serve as the foundation for all decisions related to the design, procurement, deployment, and oversight of Artificial Intelligence systems. They reflect values that protect customers, strengthen institutional trust, and ensure AI systems support the long-term stability of the Bank. The SAFE-AI principles are; Secure, Accountable, Fair, Explainable, Africa-centred, and Impact-Driven.

Secure

Every AI system must be designed and operated in a way that prevents unauthorised access, manipulation, or misuse. Security protections must be applied to the data used to train AI systems, the models themselves, and any outputs they produce. Security is not treated as a one-off requirement but as a continuous obligation through the entire life cycle of the AI system.

Accountable

The Bank remains responsible for the outcomes of all AI tools it uses, even when those tools are provided by external vendors. No AI system may operate without a clearly assigned owner within the Bank who is accountable for its performance, monitoring, updates, and reporting obligations. Staff should understand that AI tools assist decision-making, but they do not replace the Bank's accountability.

Fair

AI systems must treat all customers and staff fairly. They should not make decisions that discriminate against individuals or groups based on factors that are unlawful or irrelevant. Any automated decision-making tool must be tested to detect potential bias, and corrective measures must be implemented when such bias is identified. Fairness is not limited to regulatory compliance but extends to the Bank's reputation and ethical responsibility.

Explainable

The Bank must ensure that the logic behind its AI systems can be understood by staff, regulators, and customers when required. Even if an AI model is complex, the Bank should be able to provide meaningful explanations for how outputs are generated. Explainability builds customer trust, strengthens regulatory compliance, and helps staff make informed decisions when working with automated systems.

Africa-Centred

AI systems used in Ghana must be sensitive to local context. Data used to train systems should reflect Ghanaian realities where possible, and the design of AI solutions should consider local languages, cultural norms, socio-economic patterns, and financial behaviours. This approach reduces inaccuracies and ensures the technology serves the people it is meant to support.

Impact-Driven

AI adoption within the Bank should create measurable value, either through improved efficiency, stronger risk management, better customer experience, or increased operational resilience. The Bank commits to avoiding "technology for technology's sake." Every AI tool must demonstrate a clear purpose, measurable benefit, and alignment with the strategic goals of the Bank.

Together, these SAFE-AI Principles guide the Bank's entire approach to AI governance. They represent both an ethical foundation and a practical standard for evaluating all AI-related decisions.

5. AI RISKS IN BANKING

Artificial Intelligence brings significant benefits to financial institutions, but it also introduces unique risks that must be managed with care. The Bank recognises that AI-related risks can affect operations, customers, compliance, security, and the Bank's reputation. These risks are not abstract; they manifest through real operational scenarios such as incorrect credit decisions, fraudulent use of AI tools, and unauthorised sharing of customer information.

Risk of Inaccurate or Misleading Outputs

AI systems may produce outputs that appear confident but are factually wrong. This is especially common with generative AI tools, which may fabricate content. In lending or fraud detection, such inaccuracies can lead to wrongful customer decisions, financial losses, or internal misjudgements.

Bias and Unfair Decision-Making

If the data used to train an AI system contains historical bias, the system may reproduce or amplify that bias. In the banking context, this can affect credit assessments, risk scoring, or customer categorisation. The Bank must regularly test for and correct any emerging bias.

Data Protection Risks

AI systems often rely on large volumes of data, including personal information. Poorly managed AI systems may collect more data than necessary, store data insecurely, or share it with third-party tools without proper safeguards. These practices violate the Data Protection Act and expose customers to harm.

Cybersecurity Threats

AI tools, especially those hosted in the cloud or integrated with external vendors, can become entry points for cyber attackers. Attackers may target model files, training data, or output channels to manipulate results or extract confidential information. The Bank must ensure that cybersecurity controls cover all AI components.

Reputational Risk

If customers believe that the Bank's AI systems are unfair, inaccurate, or intrusive, trust can quickly decline. Loss of trust affects customer retention, regulatory relationships, and public confidence in the Bank.

Operational Risk

AI systems may fail, drift, or behave unpredictably when conditions change. Without monitoring, an AI model that once worked accurately may gradually become unreliable. This can disrupt operations and cause internal errors.

Third-Party and Vendor Risk

External vendors providing AI tools may not always meet the Bank's standards. Weak vendor security, unclear data-handling practices, or poorly maintained AI models can introduce risk into the Bank's environment. Vendor risk must be evaluated as part of AI governance.

These risks justify a strong governance framework and demonstrate the importance of responsible AI adoption in banking.

6. GOVERNANCE AND ACCOUNTABILITY STRUCTURE

Strong governance ensures that AI is used safely, ethically, and consistently across the Bank. Governance is not limited to approving new AI tools. It includes monitoring, reporting, decision-making, and ensuring that all AI activities align with laws, the Bank's risk appetite, and industry standards.

Board of Directors

The Board provides strategic direction for the Bank's use of AI. It ensures that AI adoption supports the Bank's mission and risk appetite. The Board reviews periodic reports on AI performance, incidents, and emerging risks. It is responsible for approving this policy and any significant updates.

Senior Management

Senior Management ensures that this policy is implemented throughout the Bank. Its responsibilities include allocating resources, overseeing compliance, approving major AI systems, and ensuring that internal controls are functioning properly. Senior Management must also ensure that staff receive adequate training on AI use.

AI Oversight Committee

The Bank establishes an AI Oversight Committee composed of representatives from Risk, Compliance, IT, Data Protection, Internal Audit, and relevant operational units. This Committee evaluates proposals for new AI systems, reviews AI impact assessments, analyses risks, and

provides recommendations before deployment. It also monitors performance and oversees ongoing compliance.

Risk and Compliance Units

The Risk Department assesses how AI systems influence credit risk, operational risk, market risk, and reputational exposure. The Compliance Unit ensures that all AI activities meet regulatory and legal requirements. Both units highlight risks early and advise the Bank on mitigation strategies.

Data Protection and Information Security Units

These units ensure that AI systems process data in accordance with the Data Protection Act and the Bank's own security standards. They review data flows, evaluate the legality of processing activities, and ensure that customer information is protected throughout the AI system's life cycle.

Internal Audit

Internal Audit provides independent assurance by reviewing whether AI systems, processes, and controls comply with this policy. It assesses whether risk mitigation measures are functioning effectively and reports deficiencies to AI Oversight Committee.

System and Process Owners

Each AI system must have a designated owner within the Bank. This owner is responsible for monitoring system performance, maintaining documentation, escalating issues, and ensuring compliance with this policy.

All Staff

Every staff member has a responsibility to use AI systems appropriately, protect customer and Bank information, and report incidents or suspicious behaviour. Staff must follow all guidance provided under the Staff AI Usage section of this policy.

7. AI ADOPTION AND OPERATIONAL MANUAL

Artificial Intelligence is most valuable when it is adopted in a deliberate, structured, and risk-aware manner. This section outlines the steps the Bank must follow to ensure AI systems are implemented safely, ethically, and effectively. It integrates practical operational guidance with the Bank's governance and risk management framework.

7.1 Identifying Use Cases

Before adopting an AI system, the Bank must clearly define the problem the system will address. Use cases must be aligned with strategic objectives, operational needs, or regulatory

requirements. Examples include automating customer inquiries, enhancing fraud detection, improving loan decision-making, or monitoring transactions for unusual patterns.

Each proposed AI use case should be assessed for potential risks, benefits, and impact on customers and the Bank's operations. High-risk applications, particularly those affecting financial decision-making or customer outcomes, require enhanced scrutiny.

7.2 Conducting Impact Assessments

An AI Impact Assessment (AIIA) must be completed for all AI systems prior to deployment. The assessment should evaluate potential operational, financial, reputational, ethical, and legal risks. This includes analyzing data sources, system logic, output reliability, and any potential for biased decision-making.

The outcome of the impact assessment informs the risk classification of the AI system and the controls required to mitigate potential issues. Systems classified as high-risk may require additional approvals from Senior Management and the AI Oversight Committee.

7.3 Risk Assessment and Classification

Each AI system must undergo a formal risk assessment, documenting potential hazards, likelihood, impact, and mitigation measures. Risk assessment covers operational risk, cybersecurity, data protection, and regulatory compliance. Based on this assessment, the system will be categorized as low, medium, or high risk. This classification determines the level of monitoring, reporting, and internal approvals required.

7.4 Approval and Procurement

No AI system may be procured or deployed without formal approval. For internally developed systems, proposals must be reviewed by the AI Oversight Committee. For third-party solutions, vendor due diligence must be completed to ensure compliance with security, data protection, and operational standards. Approval processes must be documented and retained for audit purposes.

7.5 Deployment and Monitoring

After approval, the system should be implemented according to a controlled deployment plan. Staff must receive training on system use, limitations, and escalation procedures. Systems should be continuously monitored to ensure performance, accuracy, fairness, and security. Any unexpected behavior or deviation from expected results must be promptly investigated and reported.

7.6 Review and Updates

AI systems must be periodically reviewed to ensure they continue to meet business objectives, regulatory requirements, and ethical standards. Changes in operational context, data sources, or

regulatory guidance may necessitate updates or recalibration of the system. Documentation of all updates and reviews must be maintained for accountability.

8. STAFF AI USAGE GUIDANCE

Every staff member has a responsibility to use AI systems safely and ethically. Misuse of AI can expose the Bank to legal, operational, and reputational risks. This section provides clear guidance on staff responsibilities and outlines procedures for reporting concerns.

8.1 Acceptable Uses

Staff may use AI systems to support operational efficiency, enhance customer service, assist in analysis, or provide insights that improve decision-making. AI may also be used for administrative tasks, research, or educational purposes within the Bank. Staff should always consider the reliability of AI outputs and exercise professional judgment when acting on AI-generated information.

8.2 Prohibited Uses

Staff are prohibited from using AI to process sensitive personal data without authorization, make final financial decisions without oversight, generate misleading or inaccurate information, or circumvent internal controls. The use of unapproved external AI tools is also forbidden, particularly for tasks involving customer data or financial transactions.

8.3 Data Handling and Confidentiality

When interacting with AI systems, staff must maintain strict confidentiality of customer and Bank information. Data entered into AI systems should be limited to what is necessary for the task and should comply with the Bank's data protection and security policies. Staff must avoid sharing confidential information with external AI platforms unless explicitly authorised.

8.4 AI Tools Register

The Bank will maintain a central AI Tools Register. This register will document all AI systems approved for use, including internal and third-party tools. Staff must record any AI tool they intend to use and obtain the necessary approvals before adoption. This ensures transparency, accountability, and effective monitoring of all AI activities.

8.5 Reporting Concerns

Staff are expected to report any irregularities, errors, misuse, or security concerns related to AI systems immediately to their line manager or the AI Oversight Committee. Reporting should follow established incident management protocols and ensures the Bank can respond quickly to risks.

9. DATA PROTECTION AND INFORMATION SECURITY CONTROLS

Protecting data is central to AI governance. AI systems often process large volumes of sensitive information, including personal customer data, transactional records, and internal operational data. Strong data protection and security practices reduce risk and ensure compliance with regulatory obligations.

9.1 Lawful and Purpose-Limited Data Use

AI systems must only process data for legitimate purposes directly related to the Bank's operations. Data should be accurate, relevant, and limited to what is necessary for the AI system to function. Personal data must be handled in accordance with the Data Protection Act and any customer consent agreements.

9.2 Data Minimization and Retention

The Bank will limit the collection, storage, and use of data to the minimum required for the AI system's function. Retention policies must define how long data is kept and when it will be securely deleted. AI systems must not store or replicate unnecessary data.

9.3 Access Control and Encryption

Access to AI systems and their underlying data must be restricted to authorised staff. Systems should employ strong authentication, logging, and encryption to protect data from unauthorised access or breaches. Regular audits of access controls should be performed.

9.4 Vendor and Third-Party Data Safeguards

When AI systems are procured from external vendors, the Bank must ensure that these vendors comply with equivalent data protection and security standards. Contracts must clearly specify how data is handled, stored, and secured, and the Bank retains the right to audit vendor practices.

9.5 Cross-Border Data Transfers

Data sent outside Ghana, including to cloud-based AI platforms, must comply with applicable laws governing cross-border transfers. Adequate safeguards must be in place, and approvals from the Data Protection Officer or Senior Management are required before any transfer occurs.

9.6 Monitoring and Breach Reporting

All AI systems will be monitored for compliance with data protection and security requirements. Any data breaches or suspicious activity must be reported immediately following the Bank's incident response protocols. Timely reporting ensures regulatory obligations are met and risks are mitigated promptly.

10. VENDOR AND THIRD-PARTY MANAGEMENT

Artificial Intelligence systems are often developed or provided by external vendors. While such partnerships can bring expertise, innovation, and efficiency, they also introduce risk. The Bank must maintain oversight over all third-party AI solutions to ensure compliance, security, and ethical operation.

10.1 Vendor Risk Assessment

Before engaging a vendor, the Bank must conduct a thorough assessment. This includes evaluating the vendor's technical capabilities, security posture, regulatory compliance, and track record. Particular attention should be given to how vendors handle data, the transparency of their algorithms, and their capacity to maintain systems over time.

10.2 Procurement and Contractual Controls

All AI vendor engagements must follow the Bank's procurement policies. Contracts must clearly define roles, responsibilities, and service-level expectations. Agreements should include clauses on data protection, intellectual property, system updates, incident response, audits, and the Bank's right to terminate if standards are not met.

10.3 Ongoing Monitoring

Vendor performance must be regularly monitored. This includes reviewing system outputs, security compliance, updates, and risk reports. Vendors must promptly report incidents or anomalies affecting the Bank's systems. The AI Oversight Committee, in coordination with Risk and Compliance units, will periodically review vendor adherence to these standards.

10.4 Offboarding and Continuity Planning

The Bank must have clear plans for offboarding a vendor or discontinuing an AI system. This includes secure retrieval or destruction of data, transfer of operational responsibilities, and ensuring continuity of critical services. Vendor transitions must be documented and approved by Senior Management.

11. VERIFYING AI-GENERATED OUTPUTS

AI systems do not replace human judgment. Outputs generated by AI must be carefully evaluated to ensure accuracy, fairness, and reliability. Verification of AI outputs is a critical control to prevent errors, fraud, or misinformed decision-making.

11.1 Accuracy and Reliability Checks

Staff must validate AI outputs against reliable sources before taking action based on them. For example, transaction alerts, credit scoring recommendations, or customer-facing communications must be cross-checked for accuracy and consistency.

11.2 Human Oversight

High-stakes decisions, such as credit approvals, fraud investigations, or regulatory reporting, require human review. AI systems should provide insights to support decisions, but final responsibility lies with designated staff or management. Human oversight ensures accountability and prevents blind reliance on automated outputs.

11.3 Documentation of Verification

All verification activities must be documented. This includes recording the process used to assess AI outputs, the findings, and any corrective measures taken. Documentation ensures traceability and supports internal and external audits.

11.4 Escalation Procedures

If AI outputs are found to be inaccurate, biased, or suspicious, the issue must be escalated immediately to line managers, the AI Oversight Committee, or relevant Risk and Compliance units. Prompt escalation ensures rapid mitigation of potential harm.

12. TEMPLATES AND TOOLS

To support effective AI governance, the Bank will provide standard templates and tools for staff and management. These documents ensure consistency, accountability, and compliance throughout the AI lifecycle.

12.1 AI Impact Assessment Template (AIIA)

This template guides staff in evaluating the potential operational, legal, ethical, and reputational impacts of an AI system before deployment. It includes sections for risk identification, data sources, mitigation measures, and final approval by the AI Oversight Committee.

12.2 AI Risk Assessment Template (AIRA)

The AI Risk Assessment template provides a structured framework for documenting risks associated with AI systems. It includes categories for operational, cybersecurity, data protection, and reputational risks, along with risk ratings, controls, and monitoring plans.

12.3 Vendor Due Diligence Template

This tool guides staff through evaluating AI vendors. It covers technical capability, security, compliance, transparency, contractual obligations, and post-deployment monitoring. Using this template ensures all vendor engagements meet the Bank's standards.

12.4 Staff AI Usage Declaration & Tools Register

The Bank maintains a central register documenting all AI tools approved for use. Staff must submit any intended AI tool for approval and declaration. This register facilitates monitoring, accountability, and compliance with internal and external requirements.

13. INCIDENT REPORTING AND BREACH HANDLING

Artificial Intelligence systems, like any technology, may experience failures, generate errors, or be subject to misuse. Prompt and structured reporting of incidents ensures that the Bank can respond effectively, mitigate harm, and comply with regulatory obligations.

13.1 AI-Related Incident Categories

AI incidents include, but are not limited to:

- Inaccurate outputs leading to erroneous decisions
- Biased or discriminatory AI behaviour
- Data breaches or unauthorised access involving AI systems
- Vendor system failures affecting operations
- Security incidents targeting AI models or data
- Misuse of AI tools by staff or external parties

13.2 Reporting Timelines

All incidents must be reported as soon as they are detected. Minor incidents should be reported within 24 hours, while major incidents affecting customers, compliance, or operations must be escalated immediately to the AI Oversight Committee and relevant senior management.

13.3 Roles and Communication Pathways

- **Staff:** Responsible for immediately reporting anomalies or misuse of AI to their line manager or directly to the AI Oversight Committee.
- **Line Managers:** Document the incident, ensure containment, and escalate if necessary.
- **AI Oversight Committee**: Evaluates the incident, coordinates investigation, and recommends mitigation or corrective action.
- **Risk and Compliance Units**: Assess legal, regulatory, and operational impact and notify regulators if required.
- **IT and Cybersecurity Teams:** Investigate technical aspects, secure systems, and implement corrective measures.

13.4 Integration with Cybersecurity and Business Continuity Plans

AI incident management is part of the Bank's broader cybersecurity and business continuity frameworks. Lessons learned from AI-related incidents must inform updates to security protocols, AI monitoring processes, and staff training programs.

14. TRAINING AND CAPACITY BUILDING

Effective AI governance requires staff who are knowledgeable, vigilant, and capable of using AI responsibly. The Bank commits to structured and ongoing training programs to build AI competence across all relevant departments.

14.1 Mandatory Annual AI Awareness Training

All staff must complete an annual AI awareness program. This training covers:

- The Bank's AI governance policy
- Staff responsibilities in using AI systems
- Data protection and cybersecurity obligations
- Reporting procedures for incidents and anomalies

14.2 Specialised Training for Key Units

Certain departments, including IT, Risk, Compliance, and Internal Audit, require deeper, role-specific training. This includes:

- Understanding AI models and outputs
- Conducting AI risk and impact assessments
- Evaluating vendor AI solutions
- Performing verification of AI-generated outputs
- Applying regulatory and ethical compliance standards
- Training records must be maintained for audit and compliance purposes.

15. MONITORING, EVALUATION, AND REVIEW

Ongoing oversight ensures AI systems remain reliable, compliant, and aligned with the Bank's strategic objectives. Monitoring, evaluation, and review processes provide assurance that AI governance is effective and adaptive to emerging risks.

15.1 Quarterly Model Performance Review

AI systems must be evaluated at least quarterly. Reviews assess:

- Accuracy, reliability, and fairness of outputs

- Data integrity and appropriateness
- Alignment with intended business use
- Evidence of bias or unintended behaviour

Findings must be documented and shared with the AI Oversight Committee and Senior Management.

15.2 Annual Policy Review

This policy will be reviewed at least once per year to ensure it remains current with legal, regulatory, and technological developments. Updates must be approved by the Board of Directors.

15.3 AI Audit Requirements

Internal Audit will periodically assess the Bank's AI systems, governance processes, and adherence to the SAFE-AI Principles. The audit will cover risk controls, compliance, staff adherence, vendor management, and incident handling procedures.

15.4 Key Performance Indicators and Metrics

To measure the effectiveness of AI governance, the Bank will track:

- Number and severity of AI incidents reported
- Compliance with AI training requirements
- Frequency and outcomes of model performance reviews
- Timeliness of risk assessment and approvals
- Vendor compliance and service-level adherence

These metrics will inform decision-making, continuous improvement, and reporting to Senior Management and the Board.