Building Nepal's Future-Ready Financial Sector

A Strategic Guide to the Nepal Rastra Bank Artificial Intelligence Guidelines

Nepal Rastra Bank | Banks & Financial Institutions Regulation Department | December, 2025

The Strategic Imperative of AI in Nepalese Finance

Artificial Intelligence is rapidly reshaping the financial landscape. To harness its benefits while safeguarding stability, Nepal Rastra Bank has issued comprehensive guidelines following the Monetary Policy for FY 2024/25. This presentation outlines a strategic framework for responsible AI adoption.

The Opportunity

Leverage AI to enhance efficiency, innovation, and customer experience.

The Challenge

Proactively manage operational, ethical, model, and systemic risks.

The Framework

A structured approach built on Four Foundational Pillars: Governance, Risk Management, Ethics, and Operations.

The Action

Your immediate priorities are to establish clear governance, classify AI systems by risk, and prepare for new reporting standards.

A Framework for Responsible Innovation

These guidelines are designed to steer NRB-licensed institutions toward the responsible, transparent, and ethical use of AI. The goal is to build a competitive and inclusive financial sector for all.

1

Promote Innovation & Resilience

Adopt AI to enhance efficiency and customer experience while ensuring financial stability and operational resilience.

2

Ensure Fairness & Accountability

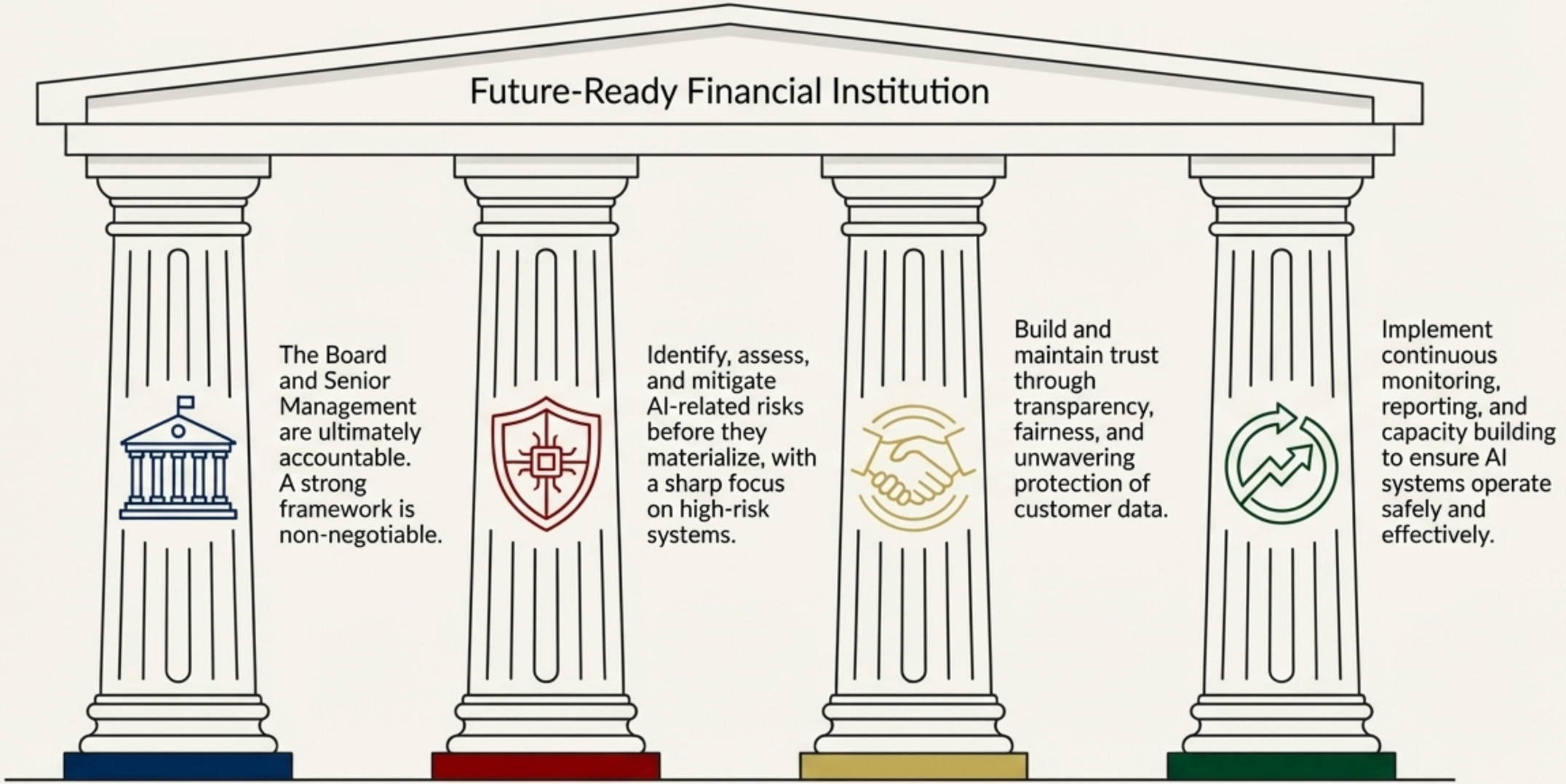
Uphold customer rights, protect data privacy, and prevent discriminatory or unethical outcomes.

3

Mitigate Core Risks

Establish robust governance to manage operational, ethical, systemic, model, and cyber risks associated with AI.

The Blueprint: Four Pillars of a Robust AI Strategy



Pillar 1: Governance & Accountability Starts at the Top

The Board of Directors and Senior Management remain ultimately accountable for the outcomes and decisions generated by the institution's AI systems.

Board of Directors' Responsibilities

- ✓ Define AI risk tolerance within the overall risk framework.
- ✓ Set the strategic direction for AI adoption.
- ✓ Establish robust governance structures with clear roles.
- ✓ Ensure implementation of ethical and transparent practices.

Senior Management's Responsibilities

- ✓ Align AI usage with risk appetite and strategic goals.
- ✓ Continuously monitor the institution's dependence on AI.
- ✓ Oversee daily operations, ensuring human oversight and auditability.

Building the Governance Structure

AI Strategy & Governance Framework

Establish a comprehensive AI governance framework, approved by the Board, and integrated with the overall risk management system.

Key Components

- Clear institutional objectives for AI.
- Defined policies, procedures, and controls.
- Measures for operational resilience and business continuity.

AI Steering Committee

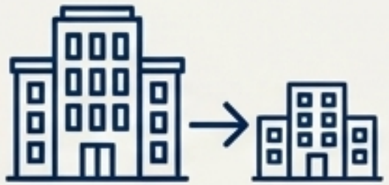
Form a cross-disciplinary AI steering committee (or assign to an existing one) with senior management and staff from business, risk, IT, legal, audit, and HR.

Managing Outsourcing Risk

Internal Use of 3rd Party Tools

Not considered outsourcing –> Institution's own governance and risk policies apply.

Outsourced AI Services



Considered outsourcing –> Requires Board approval –> Notification to NRB –> Thorough due diligence. Contracts must address data security, compliance, and auditability.

Pillar 2: Mastering AI Risk Before It Masters You

A proactive, embedded approach to risk management is essential. AI-related risks must be identified, assessed, documented, and managed within the institution's existing risk and internal control frameworks.

Key Focus Area

The initial assessment of all AI systems to classify them as 'high-risk' or 'not high-risk' is the critical first step.

Spotlight: What Defines a ‘High-Risk’ AI System?

Systems meeting these criteria pose serious threats and demand comprehensive risk management resources.

Serious Harm

Potential for significant financial loss, legal liabilities, or denial of essential services.

Broad Impact

Deployed at a large scale, increasing the possibility of systemic risk.

Minimal Human Oversight

Functions with limited human supervision, raising the risk of unchecked errors.

Rights Risk

Poses a risk to individual rights like privacy, fairness, and non-discrimination.

Sensitive Data Use

Processes highly sensitive data (e.g., biometric, large personal/financial datasets).

A 360° View of AI Risk Management

Model Risk Management

Rigorously test, validate, monitor, and decommission AI models throughout their entire lifecycle to ensure accuracy, reliability, and fairness.

Data Quality & Integrity

Establish robust data governance and formal data retention policies. Ensure data used for AI is accurate, complete, and up-to-date.

Cybersecurity

Protect AI systems against cyber threats in compliance with NRB's Cyber Resilience Guidelines. Implement regular penetration testing and AI-specific threat modeling.

Synthetic Media Risk

Assess and mitigate risks from AI-generated media like deepfakes by deploying detection tools and educating stakeholders.

Pillar 3: Building Trust Through Ethical & Responsible AI

The long-term success of AI in finance depends on trust. This requires a commitment to transparency in how AI is used, fairness in its outcomes, and rigorous protection of customer privacy.

Transparency and Explainability

Data Privacy and Protection

Fairness and Non-Discrimination

The Principles of Ethical AI in Practice

Transparency & Explainability

Explainable AI

AI decision-making must be explainable to customers, regulators, and auditors. AI-generated content must be clearly labeled.

Customer Communication

Inform customers when AI affects them and provide accessible explanations.

Audit Trails

Maintain comprehensive logs of AI decisions, aligned with international benchmarks like ISO/IEC 42001.

Data Privacy & Protection

Legal Compliance

Adhere strictly to all data protection laws, including the Privacy Act, 2075 (2018).

Data Minimization

Collect only necessary data and retain it only as long as required.

Customer Consent

Obtain explicit consent for data use and provide a clear opt-out option without denying essential services.

Fairness & Non-Discrimination

Bias Mitigation

Proactively identify and mitigate biases in AI algorithms through regular testing and monitoring.

Independent Validation

For high-risk systems, independent third-party validation is recommended to ensure fairness and accuracy.

Inclusive Design

Ensure AI systems serve all segments of the population and do not exacerbate financial exclusion.

Pillar 4: Ensuring Continuous Operational Vigilance

Deploying an AI system is the beginning, not the end. Constant monitoring, clear reporting channels, and ongoing capacity building are crucial for maintaining performance, managing incidents, and ensuring long-term compliance.

The Mechanics of Operational Vigilance

Monitoring & Re-assessment

- Continuously monitor AI system performance and impact.
- High-risk systems require more frequent monitoring and dedicated oversight plans.
- Re-assess systems when significant changes occur in functionality, operations, or the regulatory environment.

Incident & Regulatory Reporting

Incident Reporting
Report all AI-related incidents to NRB.

- **Critical:** Major failures, breaches, or significant bias.
- **Non-Critical:** Minor errors; report quarterly.

Regulatory Reporting
Submit annual reports on all AI activities using the NRB template (Annex A). Maintain detailed documentation for high-risk systems.

Capacity Building & Customer Awareness

Training
Implement adequate and regular training for board members, senior management, and employees on AI risks and technologies.

Customer Support
Educate customers on AI use and establish grievance mechanisms for AI-related complaints.

The Path Forward: Your Immediate Priorities

Compliance with these guidelines **requires immediate and structured action.**
Focus on these four areas to build your foundation for responsible AI innovation.

1. Establish Governance

Form your cross-disciplinary AI steering committee and begin drafting your **AI governance framework** for Board review.

2. Conduct an AI Inventory

Identify all current and planned AI systems. **Perform an initial assessment to classify them as "high-risk" or "not high-risk".**

3. Review Third-Party Dependencies

Scrutinize **all contracts with vendors** providing AI tools or **services** to **ensure they meet the new outsourcing and risk management requirements.**

4. Prepare for Reporting

Familiarize your risk and compliance teams with the **annual reporting template (Annex A)** and establ**ish processes for incident reporting.**

Appendix: NRB Annual Reporting Template (Overview)

A summary of the required information for the annual report on AI activities (Annex A).

Section 1: Overview of AI Systems

System Name	Technology Type	Use Case	Stage	Source (In-house/Vendor)
System A	ML/Deep Learning	Fraud Detection	Deployed	In-house
System B	NLP	Customer Service Chatbot	Pilot	Vendor X
System C	Computer Vision	Identity Verification	Development	Vendor Y

Section 3: Risk Management Measures

	Data Privacy	Bias Monitoring	Model Validation	Explainability	Human Oversight
System A	✓	✓	✓	✓	✓
System B	✓	✓	✓	No (Net fully implemented)	✓
System C	✓	✓	✓	✓	✓
System D	✓	✓	✓	✓	✓

Section 4: Governance & Compliance

AI Governance Framework in Place?	☑ Yes	☐ No
Cybersecurity Measures in Place?	☑ Yes	☐ No
AI-Related Training Programs Conducted?	☑ Yes	☐ No

Performance & Incidents

- Summary of performance metrics
- Incidents
  - Specific exand for specific examples
  - Implement valid ꝯnator examples

Future Plans

- Planned future AI initiatives
  - Implement advanced risk model
  - Expand customer support AI

**LIs are required to submit this report annually to their concerned supervision department at NRB.*