The New Mandate: An Integrated Strategic Framework for AI in Nepali Finance

Synthesizing Nepal Rastra Bank's Guidelines on AI, Cyber Resilience, and Data Privacy for Institutional Readiness

A STRATEGIC BRIEF FOR LICENSED INSTITUTIONS

A Cohesive Regulatory Vision for Responsible Innovation

Nepal Rastra Bank (NRB) has established a new regulatory paradigm centered on the adoption of Artificial Intelligence (AI). This is not an isolated mandate but an integrated ecosystem of guidelines.

The **AI Guidelines (2025)** provide the strategic direction, encouraging LIs to leverage AI for efficiency and innovation while ensuring stability and fairness.

This AI adoption is fundamentally supported and governed by parallel requirements in:

Our Objective: This brief synthesizes these directives into a single, actionable framework, demonstrating how to build a compliant and strategically sound AI program by integrating these core pillars.

Cyber Resilience Guidelines (2023): Establishing the security foundation required to protect AI systems and data.

The Privacy Act, 2075 (2018): Defining the legal guardrails for data usage, which is the lifeblood of AI.

IT Guidelines (2012): Providing the operational governance for technology infrastructure.

Unified Governance: Board and Senior Management Accountability

The board and senior management are ultimately accountable for the outcomes of AI systems. This responsibility now explicitly integrates cyber and data governance.

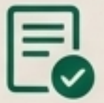
AI & Strategy (#003366)

Strategic Direction

Define the LI's AI-related risk tolerance within the overall risk management framework.

(Source: AI Guidelines, 5.1.1)

Cyber Resilience (#0A6D4D)



Framework Approval

Approve the comprehensive Cyber Resilience Framework and the AI Governance Framework, ensuring alignment with enterprise risk management.

(Source: Cyber Resilience, 17; AI Guidelines, 5.2.2)

Cyber Resilience

Resource Allocation

Ensure sufficient resources (people, technology, budget) are allocated to both AI initiatives and the underlying cyber resilience capabilities.

(Source: Cyber Resilience, 21.a)

Cyber Resilience
AI & Strategy

Expertise

Appoint at least one board member with cybersecurity expertise and ensure senior management includes members with sufficient technology-related risk expertise.

(Source: Cyber Resilience, 29.a; AI Guidelines, 5.2.2)

Cyber Resilience

Culture

Cultivate a strong culture of cyber risk awareness, where all employees understand their role in ensuring the LI's resilience.

(Source: Cyber Resilience, 25)

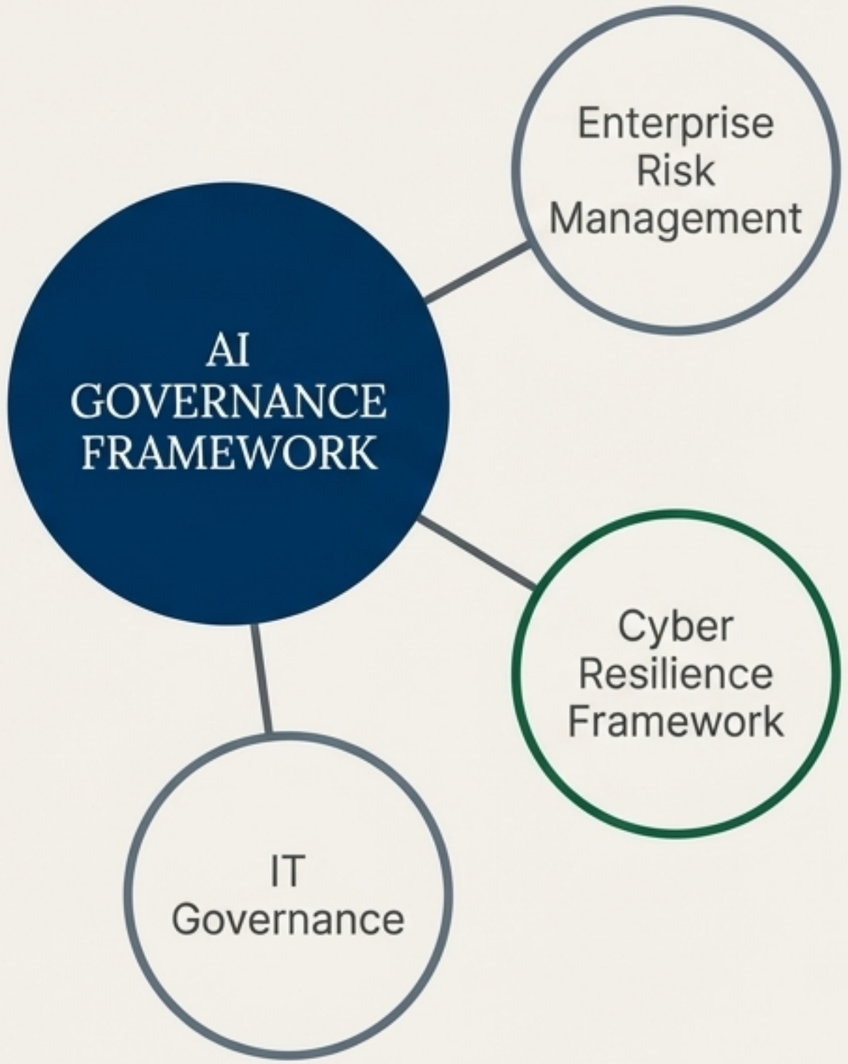
Integration Point:: Requirements from the AI Guidelines (Sec 5.1), Cyber Resilience Guidelines (Sec B.IV), and IT Guidelines (Sec 1) converge on a single, elevated standard for leadership oversight.

Structuring for Success: The Integrated AI Governance Framework

LIs must establish a comprehensive AI Governance Framework, guided by a clear AI strategy and integrated with the overall risk management system. (Source: AI Guidelines, 5.2.1)

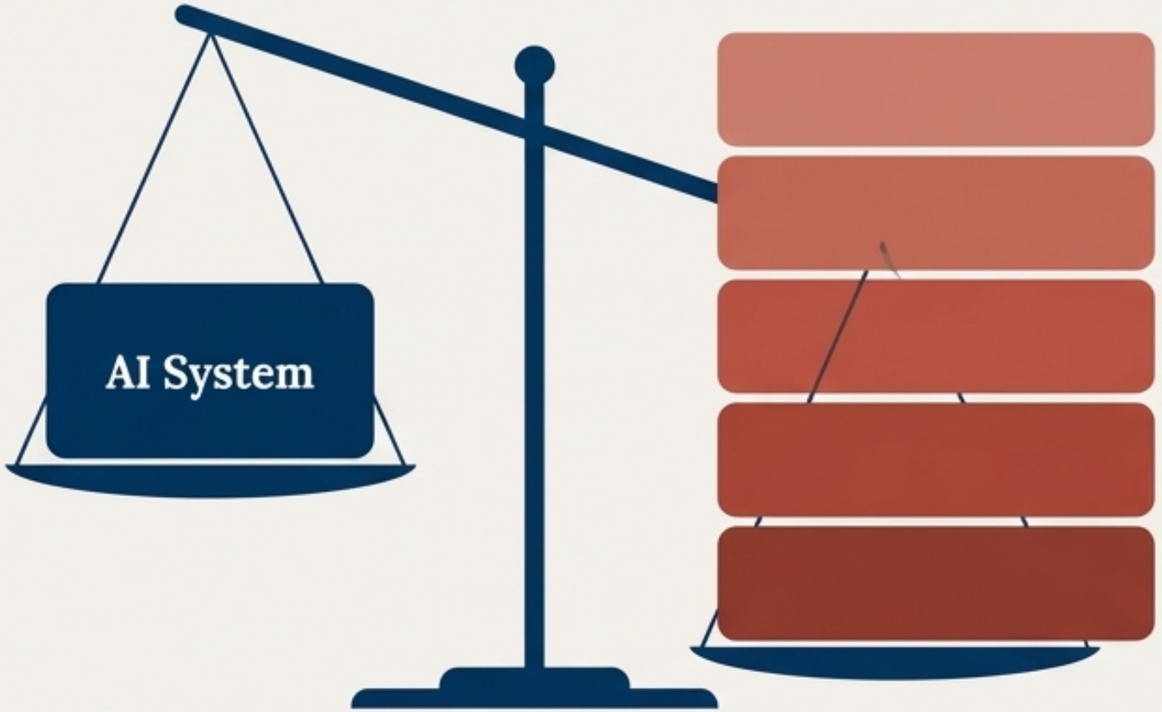
Key Structural Components

1. **Cross-Disciplinary Steering Committee**. Establish or assign a committee comprising senior management from business, risk, IT, legal, audit, and HR to guide the AI strategy. (Source: AI Guidelines, 5.2.2; Cyber Resilience, 1)
2. **Alignment with Enterprise Risk.** The AI framework must be aligned with the institution's enterprise operational risk management framework and enterprise architecture. (Source: Cyber Resilience, 9)
3. **Resilience by Design.** The framework must ensure AI systems are resilient, with measures to detect issues, restore operations, and minimize the impact of failures, supporting business continuity. (Source: AI Guidelines, 5.2.1)
4. **Policy & Procedure.** Must include well-defined policies, procedures, and controls to manage AI-related risks, specifically linking to requirements in the supporting Cyber and IT Guidelines.



The Risk Fulcrum: Identifying and Managing High-Risk AI Systems

LIs are required to conduct an initial assessment of all AI-enabled systems prior to deployment to classify them as ‘high-risk’ or ‘not high-risk.’ (Source: AI Guidelines, 6.1.1)



Serious Harm: Potential to cause 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, increasing the likelihood of unchecked errors.

Rights Risk: Poses a risk to individual rights, including privacy, fairness, and non-discrimination.

Sensitive Data Use: Processes highly sensitive data like biometric information or large personal/financial datasets.

Strategic Implication: Systems classified as high-risk demand significantly greater resources for comprehensive risk management, monitoring, and potential third-party validation.

Documentation Requirement: For systems *not* classified as high-risk, LIs must prepare and maintain a clear justification for this classification, available for regulatory review. (Source: AI Guidelines, 10.3)

The Foundation: **Securing AI with the Cyber Resilience Framework**

> "AI systems are required to be protected against cyber threats...LIs are required to implement robust cybersecurity measures...and ensure compliance with NRB's Cyber Resilience Guidelines." (Source: AI Guidelines, 6.4)

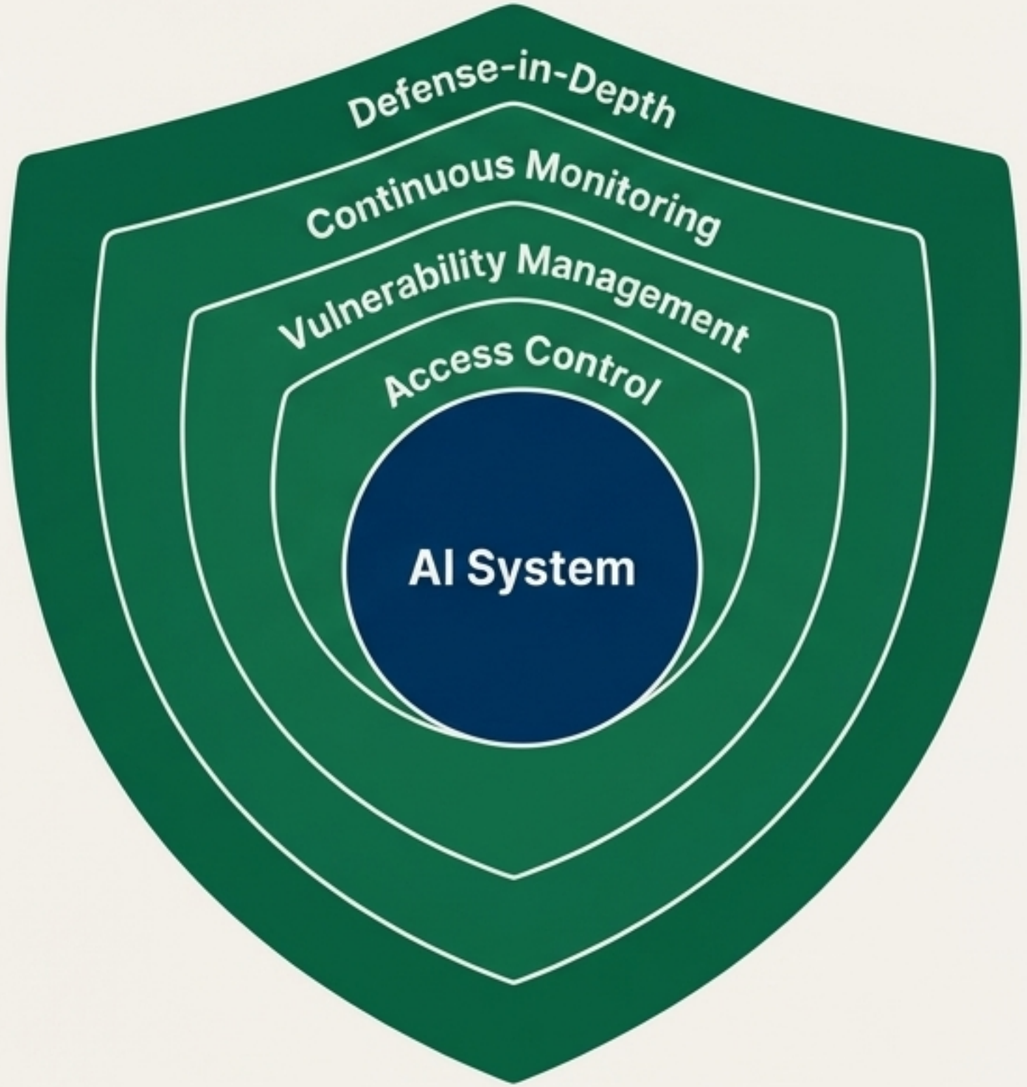
Integration with Cyber Resilience Guidelines (2023)

Defense-in-Depth: Implement multiple independent security controls (e.g., firewalls, IPS, secure network protocols) so that if one control fails, others protect the asset. (Source: Cyber Resilience, 53.f)

Vulnerability Management: Conduct regular vulnerability scanning of internal and external systems. All new deployments must undergo vulnerability assessments. (Source: Cyber Resilience, 143-147)

Access Control: Enforce principles of 'least privilege' and 'need to know.' Critical systems must require multi-factor authentication. (Source: Cyber Resilience, 71)

Continuous Monitoring: Implement automated detection systems (e.g., SIEM) to correlate network and system alerts and identify anomalous activity in near real-time. (Source: Cyber Resilience, 77.a)



As defined in Cyber Resilience Guidelines, 2023.

The Fuel and The Guardrail: Data Governance Under The Privacy Act

LIs are required to comply with all applicable data protection laws and regulations, including the Privacy Act, 2075 (2018).” (Source: AI Guidelines, 8.1)

Key Definitions from The Privacy Act, 2075

- **Personal Information:** Includes caste, ethnicity, education, address, national ID numbers, biometric information, criminal background, etc. (Source: Privacy Act, 2.c)
- **Sensitive Information:** A specific subset including caste/ethnicity, political affiliation, religious belief, physical/mental health, sexual orientation, and property details. Processing of this data is highly restricted. (Source: Privacy Act, 27.2)

Core Principles for AI Data Usage

- **Consent:** Personal data can only be collected with the consent of the concerned person. LIs must obtain explicit consent from customers before using their data in AI systems. (Source: Privacy Act, 12.2; AI Guidelines, 8.3)
- **Purpose Limitation**: Data collected shall be used *only for the purpose for which such data have been collected*. (Source: Privacy Act, 12.3)
- **Data Minimization:** Collect only the data necessary for the intended AI application and retain it only as long as required. (Source: AI Guidelines, 8.2)

Building Trust: Ensuring Fairness, Transparency, and Explainability

Bias Mitigation

LIs must take proactive measures to identify and mitigate biases in AI algorithms that could lead to unfair or discriminatory outcomes. This includes regular testing and monitoring. (Source: AI Guidelines, 9.1)

Third-Party Validation

For *high-risk* AI systems, independent third-party validation of outcomes is recommended to ensure fairness and accuracy. (Source: AI Guidelines, 9.1)

Explainable AI (XAI)

Decision-making processes of AI systems must be explainable in a manner that is understandable to stakeholders, customers, regulators, and auditors. (Source: AI Guidelines, 7.1)

Customer Communication

Customers must be informed when AI is used in decisions affecting them. AI-generated content must be clearly labeled, and AI usage during customer interactions must be disclosed. (Source: AI Guidelines, 7.2)

Comprehensive Audit Trails

Maintain comprehensive logs of AI decision-making processes. These should align with international benchmarks like ISO/IEC 42001 to support transparency and governance. (Source: AI Guidelines, 7.3)

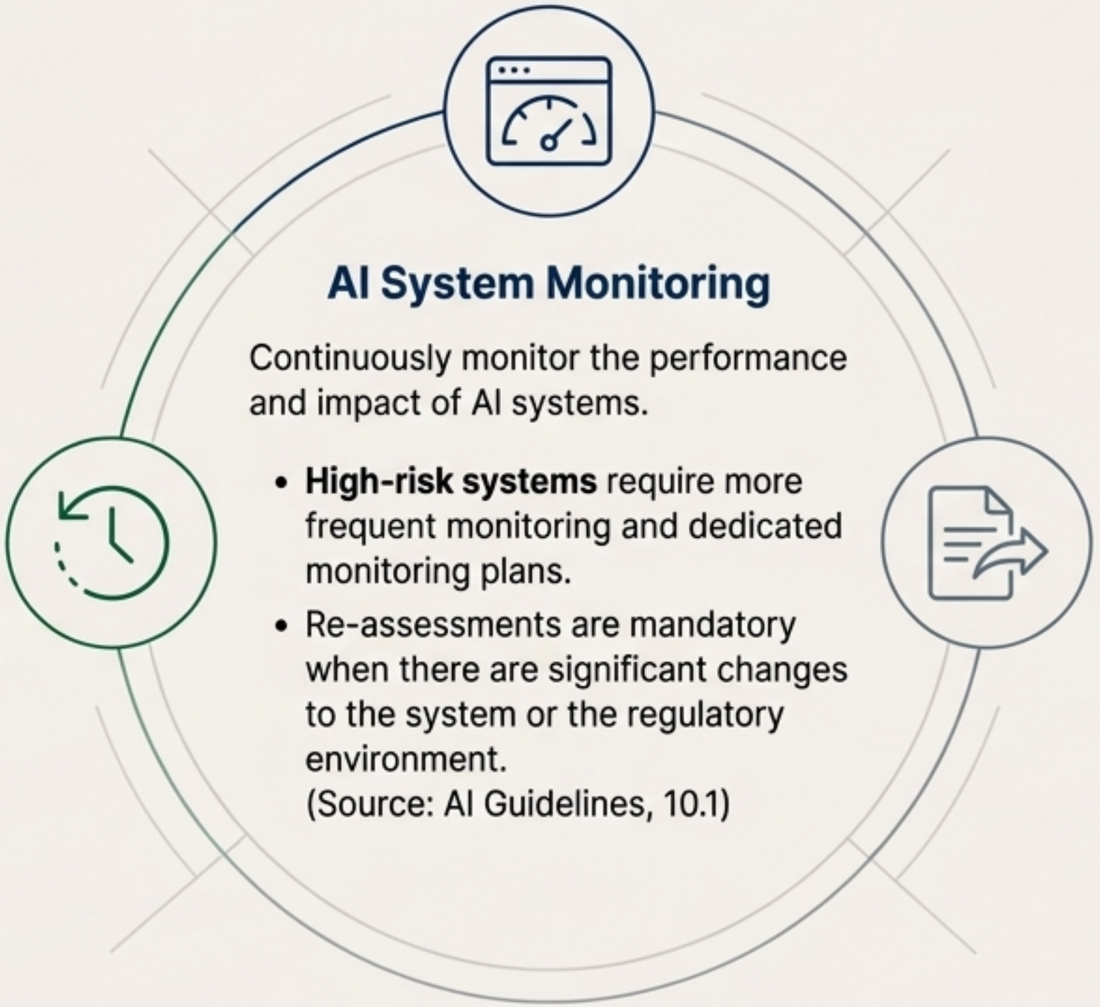
Operational Vigilance: Monitoring, Reporting, and Incident Response

Recovery and Resumption

While the AI guidelines focus on reporting, the **Cyber Resilience Guidelines** set the operational standard...

LIs must be able to resume critical operations within two hours of a disruption (the "two-hour RTO"). (Source: Cyber Resilience, 95)

This capability must be tested against extreme but plausible scenarios, including those involving AI system failure or compromise.



AI System Monitoring

Continuously monitor the performance and impact of AI systems.

- **High-risk systems** require more frequent monitoring and dedicated monitoring plans.
- Re-assessments are mandatory when there are significant changes to the system or the regulatory environment.
  (Source: AI Guidelines, 10.1)

Incident Reporting Integration

AI-related incidents (both critical and non-critical) must be reported to NRB's supervision department. (Source: AI Guidelines, 10.2)

This process must align with the broader incident response framework detailed in the **Cyber Resilience Guidelines (Sec F)** and **IT Guidelines (Sec 10)**.

Managing the Ecosystem: Outsourcing and Third-Party Risk

Defining the Boundary

Internal Use of Third-Party Tools

Using vendor AI tools for internal analysis (e.g., summarizing documents) is *not* considered outsourcing. The LI's own governance and risk policies apply. (Source: AI Guidelines, 5.3)

Outsourced AI Services

When a third party uses AI to deliver a service *to the LI*, *it is* considered outsourcing and subject to stricter controls. (Source: AI Guidelines, 5.3)

Mandatory Controls for Outsourced AI Services

1. **Due Diligence**: Conduct thorough due diligence to confirm the vendor's AI solution meets all regulatory requirements and risks are within acceptable limits. (Source: AI Guidelines, 5.3)
2. **Board Approval**: Obtain formal approval from the Board of Directors before outsourcing. (Source: AI Guidelines, 5.3)
3. **NRB Notification**: Notify the concerned supervision department of NRB. (Source: AI Guidelines, 5.3)
4. **Regulatory Access**: The outsourcing agreement must recognize the authority of NRB to carry out inspection of the service provider's systems and facilities. (Source: IT Guidelines, 5.4)
5. **Exit Strategy**: The LI's contingency planning must address the availability of alternate providers or the ability to bring the activity back in-house in an urgent situation. (Source: IT Guidelines, 5.7)

Empowering People: Capacity Building and Customer Engagement

Internal Capacity Building

Target Audience: Provide adequate training programs for board members, senior management, and all employees involved in the AI lifecycle (design, development, deployment, management).

Content: Training must cover AI-associated risks, emerging technologies, and evolving regulations. (Source: AI Guidelines, 11)

Integration Point: This aligns with the Cyber Resilience Guidelines' mandate for specialized training for high-risk groups (e.g., system administrators) and general awareness for all staff. (Source: Cyber Resilience, 74-75)

Customer Awareness and Rights

Education: Take reasonable steps to educate customers on how AI is used and how it may influence decisions that affect them. (Source: AI Guidelines, 12)

Grievance Handling: Establish or adapt existing grievance mechanisms to handle complaints related to AI-driven decisions. The process for raising concerns must be clear to customers. (Source: AI Guidelines, 12; IT Guidelines, 4)

Dispute Resolution: Clearly publish information on the dispute resolution process, including the conditions under which loss is attributable to the bank or the customer. (Source: IT Guidelines, 4.1)

The Path Forward: An Integrated Action Plan for AI Readiness

Establish Unified Governance

Form a cross-disciplinary AI AI steering committee and ensure board-level expertise in technology and cyber risk.

Develop the Integrated Framework

Draft the AI Strategy and Governance Framework, ensuring it is explicitly linked to your existing Cyber Resilience and Enterprise Risk frameworks.

Implement a Risk-Based Assessment Process

Immediately begin classifying all current and planned AI systems as 'high-risk' or 'not high-risk' based on NRB criteria, and document all justifications.

Validate Foundational Controls

Conduct a gap analysis of your current cybersecurity and data privacy controls against the specific requirements of the Cyber Resilience Guidelines and the Privacy Act, 2075.

Launch a Comprehensive Training Program

Design and schedule training modules for the Board, senior management, and operational teams, focusing on the integrated nature of AI, cyber, and data privacy risks.