Programme on

AI/ML Red Flags: Challenges in Privacy, Security & Governance

Programme Coordinator: Dr. Mridula Verma

FEBRUARY 23 - 27, 2026

Institute for Development and Research in Banking Technology, Hyderabad

(Established by Reserve Bank of India)

Introduction

As the adoption of Artificial Intelligence (AI) and Machine Learning (ML) accelerates in the banking sector, so do the associated risks—ranging from data privacy breaches, adversarial attacks, and opaque decision-making to regulatory non-compliance. While AI-driven systems promise unprecedented efficiency and personalization, they also introduce unique vulnerabilities across the data, model, and infrastructure layers. With emerging regulations such as India's Digital Personal Data Protection Act (DPDPA) and increasing scrutiny from global regulators, it is critical for banking professionals to understand not only how to build and use AI systems, but how to govern and secure them effectively.

This Executive Development Programme is designed to equip mid-to-senior level banking professionals with an in-depth understanding of AI/ML red flags, focusing on privacy, security, compliance, and governance challenges specific to the financial ecosystem.

Objectives

- To identify and analyze critical privacy and security risks across the AI/ML lifecycle—spanning data collection, model training, deployment, and monitoring
- To provide exposure to emerging threats such as adversarial ML, model drift, and federated learning vulnerabilities in the context of banking.
- To interpret and implement regulatory expectations around responsible and ethical AI use in compliance with DPDPA, RBI, and global norms.
- To develop a risk-aware governance strategy for the secure and compliant deployment of AI/ML systems in banking operations.
- To build internal capacity for AI model validation, auditing, and incident response, ensuring operational resilience and customer trust.

Contents

- Foundations of AI Risks in Banking: Understanding the Risk Landscape of AI in Banking, Data Privacy Fundamentals in the Age of AI, Security Challenges in the AI/ML Pipeline, Responsible AI: Ethics, Fairness and Accountability
- Data-Centric Red Flags: Data Quality and Bias in AI Models, Synthetic Data, Anonymization and Re-identification Risks, Federated Learning and Split Learning: Privacy and Leakage Risks, Legal and Ethical Implications of AI-Driven Decisions
- Model-Centric Red Flags: Explainability and its Governance Importance, Adversarial Machine Learning: Threats and Countermeasures, Model Monitoring, Drift, and Retraining Challenges, Shadow AI and Unauthorized Model Use
- Infrastructure and Deployment Red Flags: Security Risks in Cloud-based AI Deployments, AI Supply Chain Security, CI/CD for ML Models: DevSecOps ChallengesGovernance, Audit, and Risk Management: AI Governance Frameworks for Banks, Risk-Based Approach to AI Model Validation and Audit, Capacity Building and Organizational Readiness for Secure AI.

Who can Participate?

Officers from IT Divisions of Banks involved in technology, risk, customer experience, and strategic planning.

End Use

By the end of the Programme, participants will be able to:

- Evaluate the AI/ML models and data pipelines in their institutions from a risk and governance perspective.
- Implement privacy-preserving techniques and adopt secure MLOps practices for AI/ML deployment in regulated environments.
- Design and institutionalize a bank-wide AI governance framework including model registries, risk classification, and audit mechanisms.
- Collaborate effectively with IT, legal, compliance, and audit teams to ensure AI/ML systems adhere to ethical, secure, and privacy-conscious practices.

Programme Coordinator

Dr. Mridula Verma, Asst. Professor. e-mail: vmridula@idrbt.ac.in.

Accommodation

Participants will be provided Air Conditioned Single Occupancy accommodation in IDRBT, Hyderabad, with all cafeteria facilities. The Participants can check-in on the evening of the day before the commencement of the programme and can check-out after completion of the programme on the same day (or) in the morning of the next day of the programme.

Fee Details

Domestic Participants from

RRBs & Coop. Banks	:	Rs. 50, 000 + Applicable GST
All other Banks & FIs	:	Rs. 65, 000 + Applicable GST

The fees for our programmes can be remitted through NEFT and the bank account details for fee payment are here under:

Account Name	:	IDRBT
Bank	:	Axis Bank Limited
Branch	:	Humayun Nagar (Mehdipatnam Ring Road) Branch,Hyderabad
Account Number	:	426010100018823
IFSC Code	:	UTIB0000426
GSTIN	:	36AAAAI0204K1Z4.

Nominations

Nominations may be sent by filling the ☞ ***Nomination Form (click to fill the form)*** latest by **FEBRUARY 07, 2026**. **Please note that no nominations will be accepted after this date**. This measure is envisaged to further improve the quality and learning outcomes of the programmes based on participants' profile and requirements.

While nominating, please provide the details of the participants (Name, Designation, Bank, Mobile No / Phone No., email address) along with the nominating authority details (Name, Designation, Bank, Mobile No / Phone No., email address, Fee billing address, GST No. of the bank).

Contact Us

Please contact our Programme Office for organizing Customized Programmes and/or any other queries related to programmes at **hunar@idrbt.ac.in** or call us on +914023294141/21.

Forthcoming Programmes of February 2026

S. No.	Programme	Date	Coordinator
1.	Intelligent Process Automation	02 - 06	Prof. V. N. Sastry & Dr. Mridla Verma
2.	Security, Scale and Access for Digital Payments (A Joint programme with NPCI)	04 - 06	Dr. Abhishek Thakur
3.	Quantum Computing	04 - 06	Dr. P. Syam Kumar
4.	Data Center Management – IT & Non-IT	09 - 13	Dr. Abhishek Thakur
5.	Containerization	09 - 11	Dr. P. Syam Kumar
6.	Customer Identity and Digital Personal Data Protection Compliance for Banks and Financial Institutions	11 - 13	Prof. V. N. Sastry
7.	Application Security & Dev-Sec-Ops	16 - 18	Dr. Abhishek Thakur & Dr. Dipanjan Roy
8.	Data Privacy and Cloud Security	16 - 20	Dr. P. Syam Kumar & Dr. Susmita Mandal
9.	End to End Implementation of AI/ML in Banking	16 - 20	Dr. V. Ravi
10.	Information Systems Controls & Audit	23 - 27	Dr. Dipanjan Roy
11.	AI/ML Red Flags: Challenges in Privacy, Security & Governance	23 - 27	Dr. Mridula Verma
12.	IT Supply Chain Risk Management	25 - 27	Dr. N. P. Dhavale

Please visit our website for more details on programmes at
https://www.idrbt.ac.in/executive-development-programmes/