

NEWSFLASH

RBI Strengthens Fraud Risk Management in Banks: Emphasizes Board Oversight, Early Detection, and Fair Practices

Background

In recent years, India has witnessed a significant rise in white-collar and corporate crimes, driven by rapid economic growth and technological advancements. These crimes, often committed by individuals in high social and professional positions, have a profound impact on our society and economy. They encompass fraud, embezzlement, bribery, insider trading, money laundering, and cybercrimes. Several factors contribute to this increase:

Technological Advancements:

The digitalization of financial transactions and corporate operations has created new opportunities for cybercrimes and financial frauds. A recent report by the Indian Cybercrime Coordination Centre (I4C) revealed that digital financial frauds accounted for a staggering INR 1.25 lakh crore over the last three years. According to the National Cybercrime Reporting Portal (NCRP), in 2023, at least INR 10,319 crore was reported to be lost by victims of digital financial fraud.

Economic Growth:

India's rapid industrial and economic development has inadvertently facilitated corporate frauds. The need for effective fraud risk management is underscored by the disappearance of companies from stock exchanges. For instance, 2750 companies vanished from the Bombay Stock Exchange, highlighting the urgency of implementing robust fraud risk management measures.

Regulatory Challenges:

Despite stringent regulations and the establishment of investigative bodies like the Serious Fraud Investigation Office (SFIO), enforcement remains a challenge due to the sophisticated and covert nature of these crimes.



Judicial Trends:

Recent court judgments have highlighted the severe impact of white-collar crimes on society and the economy. For instance, a special CBI court in Ahmedabad underscored the greater societal harm caused by white-collar crimes compared to ordinary crimes. These crimes have the potential to undermine public trust in institutions, making effective fraud risk management a critical need.

The complexity and technical nature of these crimes necessitates continuous improvements in regulatory frameworks and enforcement strategies.

The Reserve Bank of India (RBI) has issued a significant update to its Master Directions on Fraud Risk Management, underscoring the critical need for enhanced governance, oversight, and operational frameworks for fraud risk management. These guidelines are aimed at various regulated entities, including commercial banks, regional rural banks, and All India financial institutions. Here are the key aspects and implications of these revised directions:

Strengthening Governance and Oversight

The revised Master Directions place a strong emphasis on the role of the Board of Directors in the governance and oversight of fraud risk management. This approach ensures that the highest levels of management are directly accountable for the integrity and robustness of fraud risk management systems. By mandating Board-level involvement, the RBI aims to foster a culture of vigilance and proactive risk management within financial institutions, ensuring that you are always prepared to tackle potential risks.

- **Importance of Governance:** The Master Directions emphasize the need for robust governance structures within banks, including clear roles, responsibilities, and accountability mechanisms.
- **Risk Committees:** Banks should establish risk committees to oversee fraud risk management. These committees play a crucial role in setting policies, monitoring implementation, and ensuring compliance.
- **Show Cause Notice (SCN):** A detailed SCN must be issued to individuals or entities accused of fraud, including promoters and executive directors. The SCN should detail the transactions or actions leading to the fraud allegation.
- **System for SCN and Response Examination:** Banks must have a structured system for issuing SCNs and reviewing responses before declaring any entity or individual as fraudulent.
- **Reasoned Order:** Banks must serve a reasoned order to the accused, detailing the decision on whether the account is classified as fraud or not. This order should include relevant facts, responses to the SCN, and reasons for the classification.

Principle-Based Approach

The new guidelines adopt a principle-based approach, which provides a flexible yet comprehensive framework for fraud risk management. This approach allows institutions to tailor their fraud risk management practices to their specific operational contexts while adhering to core principles of risk management. This flexibility is crucial for addressing the diverse and evolving nature of fraud risks in the financial sector.

Compliance with Natural Justice

A notable inclusion in the revised directions is the requirement for regulated entities to ensure compliance with the principles of natural justice before classifying individuals or entities as fraudulent. This directive aligns with the Supreme Court's judgment in the case of State Bank of India & Ors. Vs. Rajesh Agarwal & Ors., ensuring that due process is followed and rights are protected. This measure is expected to significantly enhance the fairness and transparency of fraud investigations and classifications, providing you with a sense of reassurance and confidence in the process.

Enhanced Early Warning Systems and Red Flagging

The framework for Early Warning Signals (EWS) and Red Flagging of Accounts (RFA) has been further strengthened. This enhancement aims to improve the early detection and prevention of fraud, enabling timely intervention and reporting to law enforcement agencies and supervisors. By bolstering these mechanisms, the RBI seeks to mitigate the impact of fraud and protect the financial system from potential disruptions.

Early Warning Signals (EWS): Banks must implement systems to detect unusual patterns or suspicious activities. EWS help identify potential frauds at an early stage.

Red flagging of Accounts (RFA): When certain indicators suggest possible fraud, accounts are flagged for closer scrutiny, which helps prevent further losses.

Credit Facility and Reporting of Fraud

Red-Flagged Accounts: The Directions provide procedures for classifying credit facilities or loan accounts as red-flagged accounts, which require special attention.

Third-Party Confirmation: Independent confirmation from third-party service providers and professionals is now mandatory.

Staff Accountability: The Directions address staff accountability and penal measures for lapses.

Mandate for Data Analytics and Market Intelligence

The revised directions mandate the establishment of Data Analytics and Market Intelligence Units within regulated entities. These units are tasked with leveraging advanced data analytics techniques to identify and assess fraud risks. The use of data analytics is expected to provide deeper insights into fraud patterns and trends, enabling more effective risk management strategies.

Reporting to Law Enforcement Agencies (LEAs)

- Prompt Reporting:** Banks must promptly report fraud cases to LEAs. Timely reporting is crucial for investigations and recovery efforts.
- Guidelines for Reporting:** The Directions provide clarity on reporting procedures, ensuring consistency across institutions.



Reporting to RBI and Central Fraud Registry (CFR)

RBI Reporting: Banks are required to report fraud incidents to the RBI. This central repository helps track systemic risks.

Role of CFR: The CFR aggregates fraud data, aiding in trend analysis and preventive measures.

Inclusion of Additional Financial Entities

The applicability of these Master Directions has been extended to include Regional Rural Banks, Rural Cooperative Banks, and Housing Finance Companies. This inclusion aims to promote uniformity in fraud risk management practices across different types of financial institutions, ensuring that smaller and rural-focused entities are also equipped with robust fraud prevention and detection mechanisms.

Other Instructions:

- **Legal Audit:** Large-value loan accounts require a legal audit of title documents.
- **Treatment of Fraud Accounts:** Guidelines for handling accounts classified as fraud and sold to other lenders or asset reconstruction companies.
- **Auditors' Role:** The Directions clarify the role of auditors in fraud detection and reporting.
- **Definitions:** Clear definitions of “date of occurrence,” “date of detection,” and “date of classification” are provided.
- **Reporting Non-Financial Frauds:** The Directions also address reporting cases of theft, burglary, dacoity, and robbery.

Withdrawal of Existing Circulars

With the issuance of these revised Master Directions, the RBI has withdrawn 36 existing circulars on the subject. This consolidation simplifies the regulatory framework and provides a single, comprehensive set of guidelines for fraud risk management, reducing compliance complexities for regulated entities.

Considerations for implementing the suggested changes

- Resource Allocation:** Building a robust fraud risk management framework requires investment in technology, training, and personnel. Banks, especially smaller institutions, may need to assess resource allocation carefully to ensure effective implementation.
- Balancing Efficiency and Security:** While stricter controls are necessary, it's vital to maintain an efficient customer experience. Striking a balance between security and smooth banking operations will be crucial.
- Ongoing Training:** Building a strong anti-fraud culture requires continuous employee training. Regular updates on emerging fraud tactics and best practices are essential for all staff.



Conclusion

The revised Master Directions on Fraud Risk Management issued by the RBI on 15 July 2024 represent a significant step towards enhancing the resilience and integrity of the Indian financial system. By focusing on governance, early detection, data analytics, and compliance with natural justice, these guidelines aim to create a robust framework for preventing and managing fraud risks. The inclusion of a wider range of financial entities ensures that the benefits of these enhanced practices are broadly distributed, contributing to a more secure and trustworthy financial environment.

NOIDA

(Delhi NCR - Corporate Office) A-109, Sector - 136,
Noida - 201304, India
T: +91 120 2598000

GURUGRAM

001-005, Emaar Digital Greens Tower-A 10th Floor, Golf
Course Extension Road, Sector 61, Gurgaon-122102
T: +91 0124 430 1551

CHENNAI

Prestige Palladium Bayan,
Level 5, 129-140, Greams Road, Thousand
Lights, Chennai - 600006 T: +91 44 46549201

PUNE

3rd Floor, Park Plaza, CTS 1085,
Ganeshkhind Road, Next to Pune Central
Mall, Shivajinagar, Pune - 411005, India

DELHI

(Registered Office) B-27, Soami Nagar, New Delhi -
110017, India T: +91 120 2598000

MUMBAI

4th Floor, Iconic Tower, URMI Estate, Ganpat Rao
Kadam Marg, Lower Parel, Mumbai - 400013, India
T : +91 22 4474 3400

BENGALURU

Prestige Obelisk, Level 4, No 3 Kasturba Road,
Bengaluru - 560 001, Karnataka, India
T: +91 80 2248 4555

DEHRADUN

1st Floor, "IDA" 46 E.C. Road, Dehradun - 248001,
Uttarakhand, India T: +91 135 271 6300

www.nangia.com | query@nangia.com

Copyright © 2024, Nangia & Co LLP All rights reserved. The information contained in this communication is intended solely for knowledge purpose only and should not be construed as any professional advice or opinion. We expressly disclaim all liability for actions/inactions based on this communication.

Follow us at:



NANGIA & CO LLP

