



RBI's Master Direction on Fraud Risk Management in Banks

Key changes and their impact





Contents

01

Introduction – Master Direction on Fraud Risk Management in Banks

02

Key changes in regulations and their impact on banks


03

Key actions for banks

04

How PwC can help





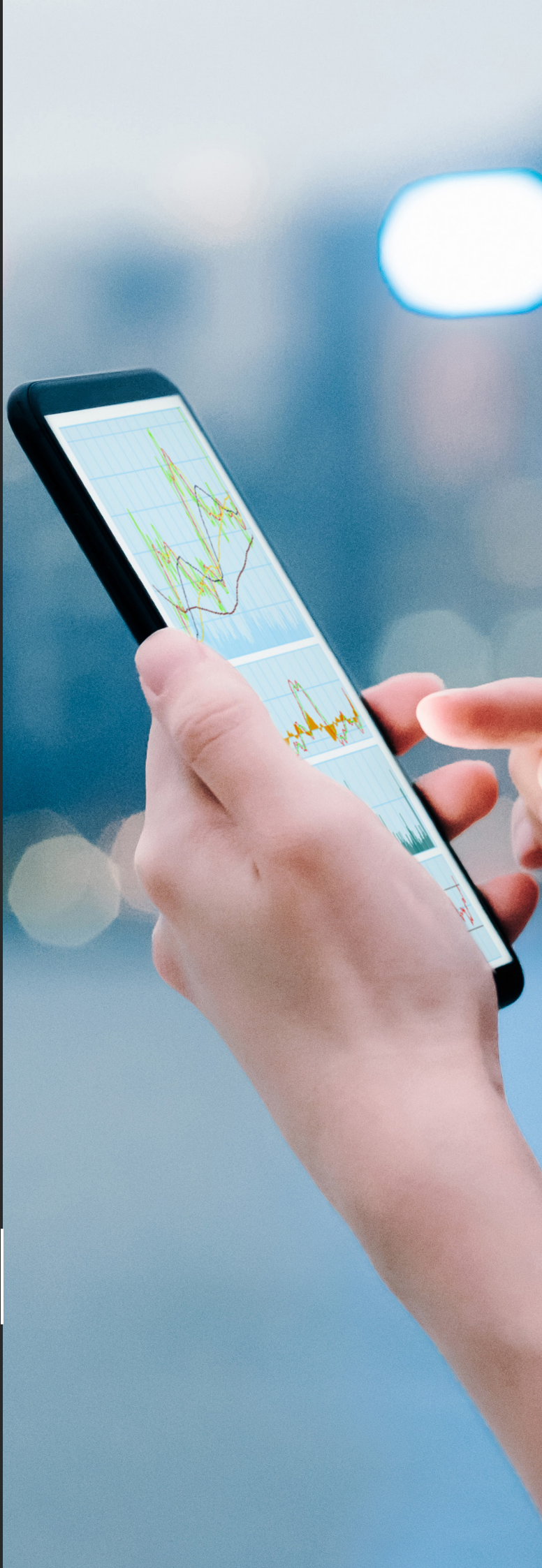
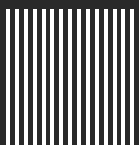
Introduction – Master Direction on Fraud Risk Management in Banks

On 15 July 2024, the Reserve Bank of India (RBI) issued the Master Direction on Fraud Risk Management in Banks, namely **Reserve Bank of India (Fraud Risk Management in Commercial Banks (including Regional Rural Banks) and All India Financial Institutions) Directions, 2024** (Ref:RBI/DOS/2024-25/118DOS.CO.FMG.SEC.No.5/23.04.001/2024-25).¹

These directions will supersede the earlier directions on the subject, namely Reserve Bank of India (Frauds - Classification and Reporting by commercial banks and select FIs) Directions 2016 (Ref.DBS.CO.CFMC.BC.No.1/23.04.001/2016-17) dated 1 July 2016 (updated as on 3 July 2017).

The directions are issued to establish a framework for banks to prevent, detect early, and promptly report fraud incidents to law enforcement agencies (LEAs), the RBI, and National Bank for Agriculture and Rural Development (NABARD), as well as to facilitate the dissemination of related information by the RBI and address associated matters.

¹ <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/118MDE97B8ED9A09B4B21BE7FDDE5F836CD09.PDF>

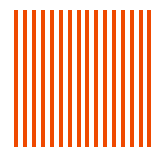




Classification of frauds as per the new master direction

| | | | |
|---|--|----|--|
| 1 | Misappropriation of funds and criminal breach of trust | 7 | Wilful falsification, destruction, alteration, mutilation of any book, electronic record, paper, writing, valuable security or account with intent to defraud* |
| 2 | Fraudulent encashment through forged instruments | 8 | Cash shortages on account of frauds* |
| 3 | Manipulation of books of accounts or through fictitious accounts and conversion of property | 9 | Fraudulent transactions involving foreign exchange |
| 4 | Cheating by concealment of facts with the intention to deceive any person and cheating by impersonation* | 10 | Fraudulent electronic banking/digital payment related transactions committed on non-banking financial companies (NBFCs)* |
| 5 | Forgery with the intention to commit fraud by making any false documents/ electronic records* | 11 | Other type of fraudulent activity not covered under any of the above |
| 6 | Fraudulent credit facilities extended for illegal gratification | | |

*These categories are newly added or updated in the Master Direction on Fraud Risk Management issued on 15 July 2024.



Key changes to the regulations and their impact on banks

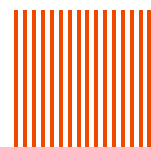
I. Governance and accountability for fraud risk management (FRM)

| Clause | Key regulations/updates to regulations | PwC's perspective |
|--------------------------------|---|---|
| Applicability | Applicability of the regulations is expanded from only scheduled commercial banks and select financial institutions (FIs) to include regional rural banks (RRBs), local area banks (LABs), corresponding new banks, Exim Bank, NABARD, National Bank for Financing Infrastructure and Development (NaBFID), National Housing Bank (NHB) and Small Industries Development Bank of India (SIDBI). | <ul style="list-style-type: none"> The expansion of the FRM regulations to RRBs, LABs, Exim Bank, etc., will enhance the FRM culture across the wider industry and promote a standardised approach to FRM. Fraudsters who could not penetrate a scheduled bank exploited vulnerabilities in systems and controls of these banks to perpetrate fraud. As such, these regulations will help lay a strong foundation for a robust FRM framework. Accountability and governance of fraud at the board level will increase as the policy will be board approved and its special committee will oversee effective implementation. Further, the committee will be headed by an independent director(s), which will dilute the influence of a bank's senior leadership in the determination of a red-flagged/fraud accounts, which was seen in many high-profile cases. |
| Focus on FRM | Increased focus on fraud prevention and FRM rather than just detection and reporting of frauds which is reflective in the change in the name of the master direction from 'classification and reporting of frauds' to 'Fraud Risk Management'. | |
| Board approved policy | Emphasis on board approved policy outlining roles and responsibilities of board/committees and senior management (SM) and containing fraud prevention and early detection measures including ensuring compliance with the principle of natural justice (issue of show cause notice [SCN]), which is a significant update to the previous circular. | <ul style="list-style-type: none"> A dedicated senior role for overall monitoring and reporting of frauds within the risk function is a progressive step in embedding and institutionalising an anti-fraud culture within banks. The responsibility of successful implementation of FRM lies with the SM. |
| Special committee of the board | The monetary threshold of INR 10 million for Special Committee of the Board for Monitoring and Follow-up of Cases of Frauds (SCBMF) is removed, and it shall now be headed by independent or non-executive directors to oversee the effectiveness of FRM. | <ul style="list-style-type: none"> The provision of the principle of natural justice allowing for serving of SCN to borrowers will provide a legitimate opportunity to borrowers to present their perspective backed by supporting arguments and documentation, if any, to banks before their account is classified as fraud. The onus will be on the lenders to carefully assess the merit of such claims before making a determination, which, if not in the borrower's interest, could be challenged in the court of law. |
| Embedding FRM in risk | Embedding FRM in the risk function with a dedicated senior-level role for overall monitoring and reporting of frauds. | |



II. Early warning signals (EWS), red flagging and Investigations

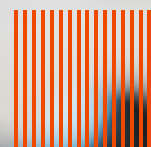
| Clause | Key regulations/updates to regulations | PwC's perspective |
|---|--|---|
| EWS and red flagging of accounts (RFA) | <ul style="list-style-type: none">• Stress on board approved EWS and RFA framework under the overall FRM policy with supervision of its effectiveness by the Risk Management Committee of the Board (RMCB)• Threshold of INR 500 million for flagging and reporting removed• EWS system integration with core banking solution that shall connect EWS to customer profile and other data• Also, EWS framework for other banking/non-credit related transactions has been introduced | <ul style="list-style-type: none">• Currently, banks have a fragmented approach towards the EWS framework with critical aspects regarding data, technology, processes and people operating in silos. There is also a lack of independence in the EWS assessment with business teams (retail/wholesale) taking views on large accounts instead of risk defeating the purpose of the framework. Embedding the EWS and RFA framework within the board approved FRM policy with RMCB supervising its effectiveness will set up a strong foundation for the EWS framework. |
| Data analytics (DA) and market intelligence (MI) unit | Set up a dedicated DA and MI unit to facilitate collection and processing of relevant information to enable early detection of fraud. This unit shall monitor both credit and non-credit transactions to identify unusual patterns and activities. | <ul style="list-style-type: none">• Inclusion of EWS for non-credit transactions is a significant change, and it will require banks to integrate early warning triggers in their existing fraud monitoring framework to identify unusual patterns and activities in transactions through digital platforms. This integration will require system/process changes, training, time and investments as EWS is currently limited to loan accounts. |
| External/internal audit of RFA | Banks will be required to appoint an external auditor or perform an internal audit for investigation of a red-flagged account. | <ul style="list-style-type: none">• While many large banks do have a DA unit, the requirement to have a dedicated 'DA and market intelligence unit' to not only collect and analyse information on loan accounts but also analyse transactions to identify unusual patterns will require investments and capability enhancements on a large scale at banks, particularly small banks such as RRBs and LABs. |
| Policy on engagement of external auditors | Policy on engagement of external auditors for RFA investigation covering due diligence, competency and track record of auditors, etc | <ul style="list-style-type: none">• Banks will be required to onboard people with field intelligence skills and experience as their own staff is not trained on these skills. |
| Classification of accounts as fraud | Completion of the process of classification as a fraud or removal of RFA status within 180 days of reporting such account | |
| Investigation of group companies | Borrowing accounts of related companies (sharing common promoters or directors) of a company whose account is identified as fraud will also be investigated for fraud by the banks involved. | |





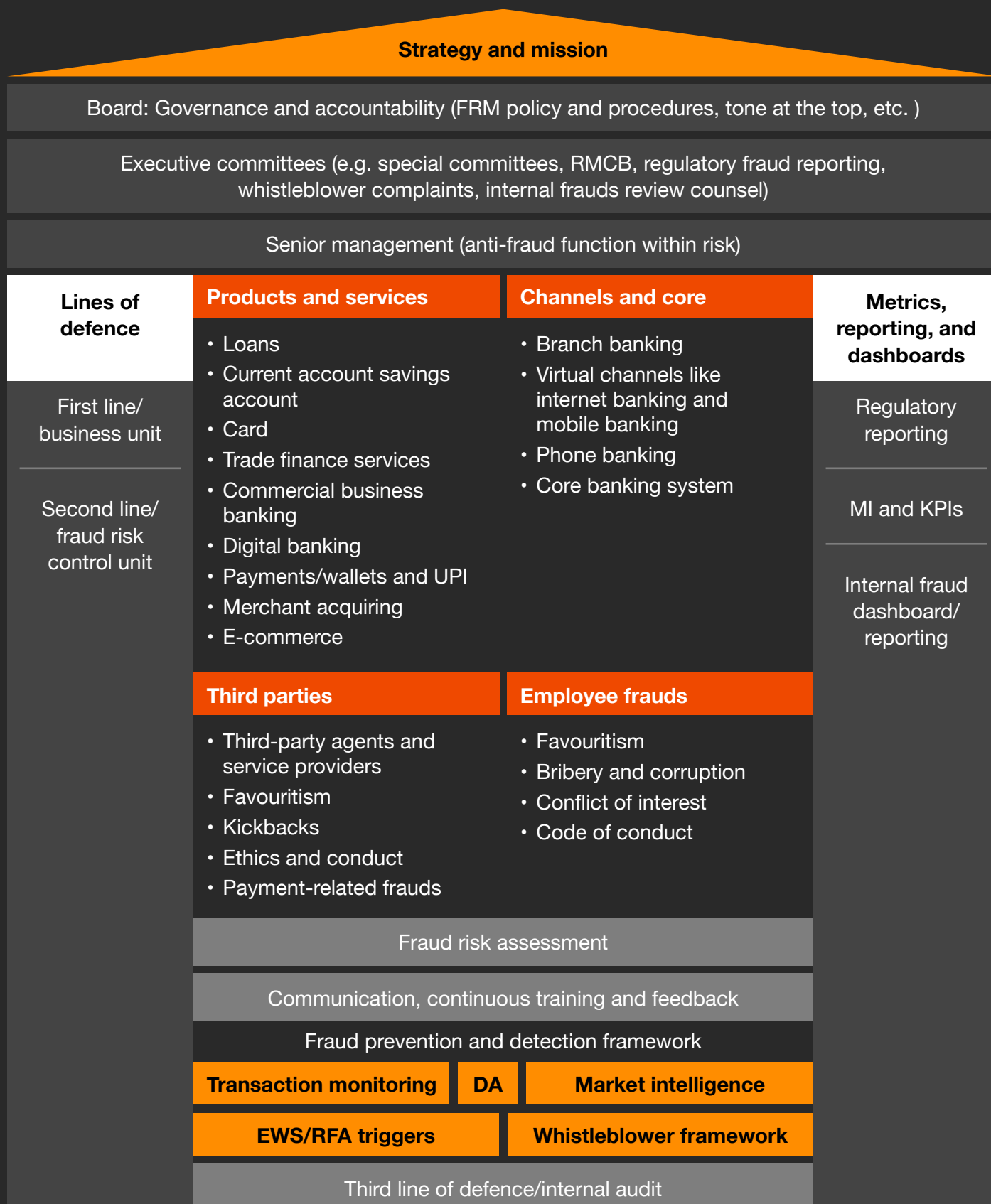
III. Fraud reporting

| Clause | Key regulations/updates to regulations | PwC's perspective |
|--|--|--|
| Reporting of group entities | Reporting of frauds committed within group entities, including domestic and overseas subsidiaries, affiliates, etc., to the RBI separately. This requirement applies regardless of whether the entity operates in the financial or non-financial sector. | <ul style="list-style-type: none">• With the introduction of reporting of frauds in non-regulated group entities of banks to the RBI, the anti-fraud governance in the group entities will likely be strengthened considering the impact it can have on the entire group. This is driven by a few recent cases of enforcements, wherein non-regulated group entities had influence in the day-to-day operations and management of the RBI regulated entity.• The fraud reporting timeline is reduced from 3 weeks to 2 weeks which will require robust processes for fraud detection and determination. This means that activities such as fraud detection, its classification and review by SM, its committees and the final determination needs to happen within 2 weeks, for which the operationalisation of the FRM framework is critical.• It was observed in many cases that banks were reporting names of people/entities who may not have been involved in the alleged fraud in their FMR reporting, which led to many senior executives/ persons being named in such returns. The amendment in the regulations to call this out will go a long way in ensuring that the anti-fraud function in banks does its due diligence before reporting such details in FMR. |
| Fraud at overseas branches | Reporting of fraud at overseas branches to the respective local law enforcement authorities in compliance with the applicable laws and regulations of the host countries | |
| Timeline of reporting | <ul style="list-style-type: none">• Reporting of each individual fraud case promptly, within 14 days from its classification, regardless of the amount involved• Notification to the Fraud Monitoring Group (FMG), Department of Supervision (DOS) and the RBI of instances involving theft, burglary, dacoity and robbery (including attempted cases), within 7 days of their occurrence | |
| Persons/entities not involved in fraud | Banks should not report persons/entities who are not involved or associated with the fraud in the FMR. | |



Key actions for banks

Effective FRM framework





Strategic Initiatives for an effective FRM



Special committee of board

Constitute an SCBMF headed by an independent director/non-executive director that shall oversee effectiveness of FRM in banks.



Board approved policy

Develop a board approved policy on FRM, clearly defining roles and responsibilities of the board/committees, SM and measures for fraud prevention and detection, including provisions on principle of natural justice.



Dedicated FRM role in risk

Appoint a senior official at the rank of at least a general manager or equivalent for monitoring and reporting of frauds.



Policy for auditors' engagement

Develop a policy on engagement of external auditors covering aspects such as due diligence, competency and track record of the auditors.



EWS framework

Set up/upgrade EWS framework by 15 Jan 2025. The EWS framework integrated with core banking should be comprehensive, incorporating both quantitative and qualitative indicators, and should provide for periodic review of the credit sanction/monitoring process.



Reporting of fraud

Comply with new reporting requirements of fraud/ RFA to LEAs and the RBI, including reporting of fraudulent transactions related to payment systems Central Payments Fraud Information Registry (CPFIR), fraud pertaining to group entities not regulated by the RBI, and frauds at an overseas group entity.



EWS for non-credit transactions

Implement EWS system to monitor other banking or non-credit related transactions.



DA and MI unit

Set up a DA and MI unit, which shall facilitate collection of relevant information to enable early detection and prevention of fraud. The unit will monitor and analyse both credit and non-credit transactions.



How PwC can help

01 Development of policy, FRM framework and training

03 Enhancement and compliance of reporting mechanism

02 EWS framework enhancement and implementation support

04 Supporting fraud prevention through DA and MI

Points to consider

- PwC can help in developing a robust FRM governance framework by benchmarking with the regulatory requirement and designing training programmes based on the updated guidelines.
- We can support in developing, enhancing and implementing EWS by reviewing the framework and scenarios, ensuring effective early fraud detection.
- Assist in meeting the revised reporting requirements, ensuring integration of relevant systems, and accurate and timely submissions.
- We can support in designing the DA and MI strategy and set up the DA and MI unit by bringing in the relevant knowledge, experience and technology.





Our accelerators: 1. Due diligence and intelligence platform

Our automated intelligence platform Prudence+ can perform due diligence and gather intelligence on individuals or entities accurately and effectively, thus complementing a bank’s EWS framework and strengthening its FRM framework.

- 1

Prudence+ is a **client-facing** workflow application built by PwC India to assist clients in **streamlining their due diligence requests**.
- 2

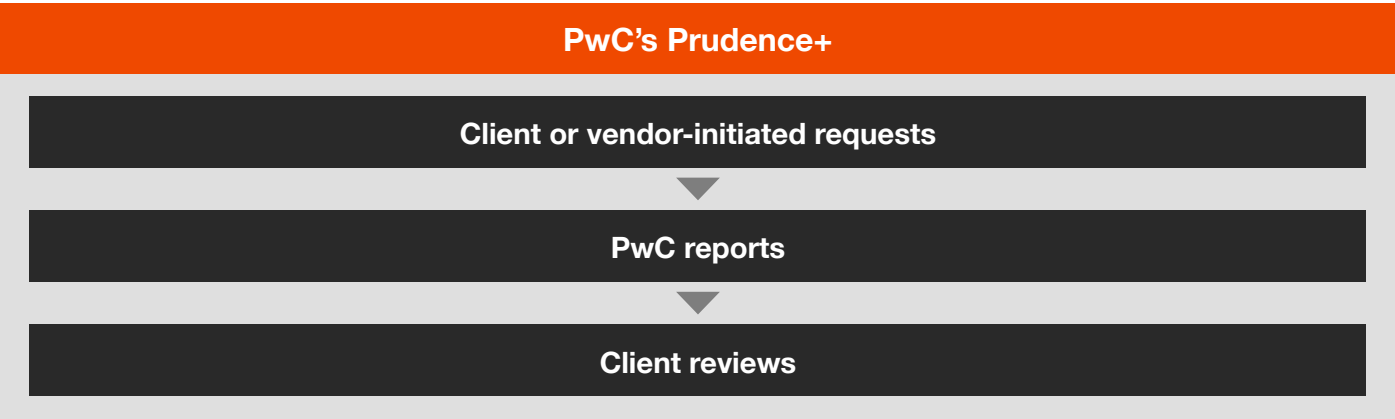
It is a web application that connects **PwC’s Intelligence team with its clients**.
- 3

Clients or vendors can submit due diligence requests by filling in key details such as target names, indicia and related documentation.
- 4

Each request **triggers a workflow** and PwC staff is intimated about the same.
- 5

Reports and supporting documentation are also uploaded onto PwC’s Prudence+ and are always available for the client to review.
- 6

It offers **audit trails and dashboards** to help PwC and its clients in tracking requests and reports.





Our accelerators: 2. Proactive fraud monitoring

Our fraud detection solution detects document and image forgery. It can be integrated with a bank's onboarding/customer relationship management (CRM), loan origination system (LOS) or other systems to detect the document frauds relating to KYC, loan documentation, employee expenses and vendor claims.

| An integrated fraud analytics platform | | | | |
|--|--|--|---|--|
| Import data from multiple sources | Business rule engine | Image and metadata analytics | PDF tampering | Visualisation |
| <ul style="list-style-type: none">• ERP and non-ERP• Internal and external• Cloud• Integrate with apps and services | <ul style="list-style-type: none">• Leverage business and policy knowledge in combination with optical character recognition (OCR)/natural language processing (NLP) capabilities for powerful rules and better exceptions generation. | <ul style="list-style-type: none">• Using AI and machine learning (ML)• Document tampering/ dedupe/ classification for scenarios of ghost billing and collusion amongst employees | <ul style="list-style-type: none">• Identify and localise instances of tampering of PDFs with the use of PDF editing services | <ul style="list-style-type: none">• Interactive dashboards and transaction-wise data• Automation of reports at designed frequencies |

The advantages



Flexible deployment options



Automated process – 100% coverage of transactions



Efficient and more accurate – better insights into fraud management/risk assessment



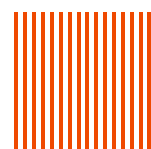
Efficient modus operandi in mitigating risks and identifying fraud typologies



Investigative efficiency – deeper insights into risks, enabling quicker resolution



Cost-effective – power of one platform



About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 360,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2024 PwC. All rights reserved.

Contact us

**Puneet Garkhel**

Partner and Forensic
Services Leader

M: +91 9820320181

E: puneet.garkhel@pwc.com

**Dhruv Chawla**

Partner, Risk Consulting

M: +(91) 8130166550

E: dhruv.chawla@pwc.com

**Induvant Tomar**

Director, Financial Crime
Compliance – Forensic Services

M: +(91) 9560833555

E: induvant.tomar@pwc.com

pwc.in

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

© 2024 PricewaterhouseCoopers Private Limited. All rights reserved.

AW/August 2024 - M&C 40148

