Internal Risk Assessment guidance for money laundering/terrorist financing risks

December 2024

kpmg.com/in

KPMG. Make the Difference.

Introduction

As per the Reserve Bank of India's KYC Master Direction, 2016[1], banks and other regulated entities (REs) are required to conduct internal risk assessments (IRA) to detect, assess, and mitigate risks associated with money laundering (ML), terrorist financing (TF), and proliferation financing (PF).

In this regard, RBI on 10 October 2024 came up with a comprehensive list of guidelines on internal risk assessment for money laundering (ML) and terrorist financing (TF) risks[2] for banks, NBFCs and regulated entities (REs) to assess and mitigate risks related to money laundering, terrorist financing, and proliferation financing across clients, countries or geographic areas, products, services, transactions, or delivery channels. The guidance note issued by the central bank lays down the foundation, methodology and follow-up actions to be taken into consideration by the REs while conducting their internal risk assessment procedures.

Key drivers for the guidance

The need for RBI to issue a guidance note on IRA stems from several key factors:

Increasing complexity of financial systems

The financial system is continuously facing more complex and evolving risks. New technologies, such as digital payments and online banking, have introduces new vulnerabilities that can be exploited for illegal financial activities.

Enhancement of operational efficiency

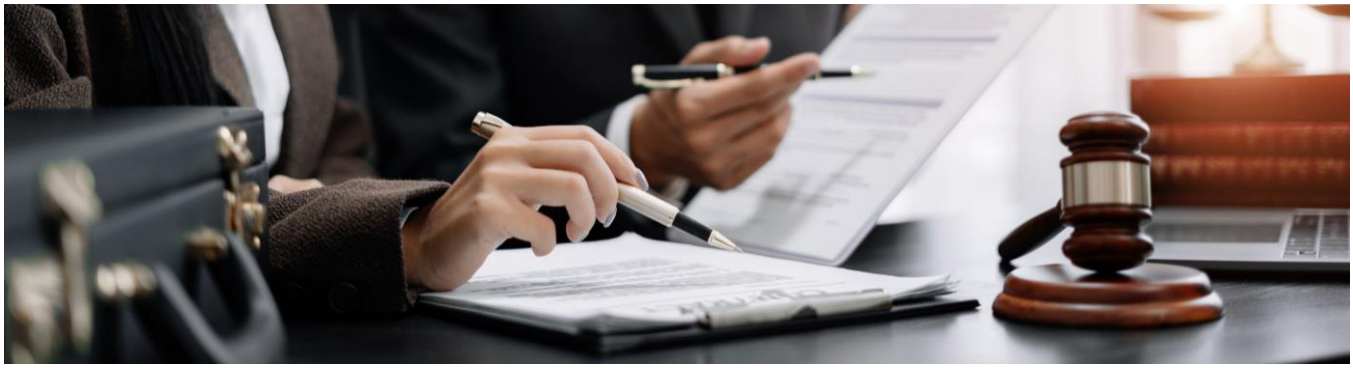
The guidance encourages institutions to regularly assess and update their risk profiles in response to emerging threats or changes in their business operations, so that they are operationally resilient in the face of evolving financial crime techniques.

Alignment with global standards

The guidance is rooted in both national regulations and international standards like the FATF recommendations and the basel committee's guidelines, ensuring that regulated entities in india can meet global expectations on AML and CFT. It emphasizes a risk-based approach (RBA) that allows entities to allocate resources effectively based on the risk profiles of their customers and products.

Sector specific risks

Different sectors such as banks, NBFCS, and payment system operators and other small financial institutions face unique ML/TF risk depending on their products and customer profiles. The guidance provides a tailored approach for these institutions to develop risk management processes that suit their business models, helping them to avoid one-size-fits-all strategy



1. Know Your Customer (KYC) Master Direction- Reserve Bank of India, 2016
2. Internal Risk Assessment Guidelines for Money Laundering/Terrorist Financing Risks- Reserve Bank of India, October 2024

Summary of the guidance

Chapter 1: Foundation of the Internal Risk Assessment

This chapter sets the tone of enterprise-wide understanding of ML/TF risk. It mandates that Regulated entities (REs) regularly conduct an Internal risk assessment (IRA) to identify, assess, and mitigate risks. The focus on the risk based approach (RBA) is crucial as it provides flexibility for REs to tailor their controls. Further, the chapter emphasis on regulatory compliance (PML Act, FATF guidelines) ensures that REs align their internal processes with global standards, fostering a more secure and compliant banking environment.

1. **Applicability of guidance:** This guidance applies to all REs including banks, NBFCs, authorised persons, Payment System Operators, etc.
2. **Risk-based approach:** At the core of this guidance note is the risk-based approach (RBA), which tailors the financial institutions' AML/CFT measures according to the specific risk levels they encounter.

   As recommendation 1 of FATF stresses, the RBA allows entities to deploy their resources more effectively and apply preventive measures that commensurate with the ML/TF/PF risks posed by the customers, in order to focus their efforts in the most optimal way.
3. **Dual-level IRA for ML/TF risks:** The guideline outlines two critical levels of risk assessment:
   - Business level assessment analyses risks inherent in the institutions' overall business model, size, and service complexity
   - Individual level risk assessment categorises customers based on their risk profiles, geographical locations, type of products etc., guiding institutions to customise their CDD efforts accordingly.

   The integration of both levels into a unified assessment ensures a holistic view of REs risk exposure since it enables the RE to understand the enterprise-wide risks.
4. **Identification and assessment of ML/TF risk factors:** The guidance note gives an indicative list of inherent and control risk factors that the REs need to consider while identifying and assessing the ML/TF risks they are exposed to. Following are a few of them enlisted in the note:

Inherent risk factors

- Nature, scale, diversity and complexity of their business diam no
- Customer profile and type of products/services offered to them
- The volume and size of their transactions
- Type of customers-individual/legal entity/legal arrangement including trusts.
- Type of on-boarding- face-to-face or non-face-to-face

Control risk factors

- Ability or lack thereof, to obtain necessary information in case of wire transfers
- The jurisdictions the REs are exposed to, especially jurisdictions with relatively higher level of corruption, and/or deficient AML/CFT controls
- Distribution channels such as ATMs, business correspondents, mobile applications etc.
- Dependance on third parties or unregulated intermediaries
- Internal audit and regulatory observations

This granular assessment of risk factors help REs to determine the level of CDD that is to be applied in specific situations, and to particular types of customers, products, services, and delivery channels.

5. **Consideration of internal and external sources:** REs are suggested to use information from internal and external sources to identify all relevant risk factors.
    - Internal sources include information from specific business relevant information and other related verticals of REs such as fraud/cyber risk management verticals
    - External sources include national risk assessment (NRA) report of the Government of India; reports/public statements/press releases published by inter-governmental international organisations such as FATF, etc., guidance and advisories from government authorities, FIU-INDIA, Reserve Bank, etc.
6. **Avoid a siloed approach:** RBI also stressed the need to avoid a siloed approach where only the AML team is involved in the IRA exercise. A cross functional approach must be followed where the IRA team may include officials from the product/service owner department, internal audit function, compliance function, etc. to properly the associated ML/TF risks.
7. **Data driven methodology:** REs are encouraged to adopt a data-oriented, objective approach to prevent any form of bias in the IRA process. Ensuring the quality of data inputs is critical to producing meaningful and useful results.
8. **IRA report:** The guidance also specifies maintaining an IRA report to enable the stakeholders within the RE to have a comprehensive view of the outcomes of the report. It also provides an indicative list of sections that need to be included in the report.

Chapter 2: Methodology and quantification of ML/TF Risk assessment and control measures

This chapter introduces a detailed methodological framework for conducting the IRA. The focus on inherent risks, combined with the evaluation of internal controls and calculation of residual risk, represents a sophisticated and quantifiable approach to risk management. This chapter provides a granular approach to risk assessment, ensuring REs adopt a structured and data driven approach. The clear breakdown of inherent, internal, and residual risks enables financial institutions to have a more precise risk profile, leading to better decision making.

1. **Methodology:** While the guideline acknowledges numerous ways in which REs can conduct IRA exercise, it elaborates on the conventional methodology of identifying inherent risks, applying internal controls, and determining residual risks. Steps include defining risk factors, collecting data, assigning weights, calculating risk scores, identification of internal controls and calculation of residual risks.
2. **Risk factors:** Further the guideline also provides an indicative list of risk factors to be considered while conducting an IRA:
    - Customer risk factors: Type of customer, ownership complexity, PEP status, etc
    - Geographic risk factors: Jurisdictions associated with customers, beneficial owners and REs
    - Product/service risk factors: Transparency of transactions, complexity and value/size of products, services, or transactions
    - Delivery channel risk factors: Non-face-to-face customer onboarding, use intermediaries, etc

    REs are provided the flexibility to examine and define other risk factors based on the introduction of new products/ services, enforcements or supervisory actions, changes in internal systems deployed for AML alerts etc.
3. **Assigning weights to risk factors:** While the standard practice is to assign a score to each risk factor/sub-risk factor, the new guideline additionally requires the REs to assign weights based on the contribution of each risk factor to the overall ML/TF risk. This weighted system ensures that REs can prioritise risk factors that pose the greatest threat.
4. **Risk classification:** Risks are categorised into high, medium, or low depending on the nature of the business and the level of risk each factor generates.
5. **Internal controls:** The effectiveness of an RE's risk management depends heavily on its internal controls, such as governance structures, staff integrity, monitoring systems, record keeping, screening etc. REs are also advised to evaluate the effectiveness of internal controls and assign weights.
6. **Residual risk:** The internal controls directly impact the residual risks i.e., after applying mitigating controls to inherent risks, the residual risk is calculated. The guidance emphasises on reducing the inherent ML/TF risks or strengthening internal controls to significantly reduce residual risk.

Chapter 3: Follow-up actions and incorporation of Proliferation Financing risk in IRA

This chapter introduces a detailed methodological framework for conducting the IRA. The focus on inherent risks, combined with the evaluation of internal controls and calculation of residual risk, represents a sophisticated and quantifiable approach to risk management. This chapter provides a granular approach to risk assessment, ensuring REs adopt a structured and data driven approach. The clear breakdown of inherent, internal, and residual risks enables financial institutions to have a more precise risk profile, leading to better decision making.

1. **Communication of IRA results:** The results of the IRA should be reported to the board, or committee of the board, and relevant stakeholders within the organisation to ensure that findings are acted upon effectively.
2. **Follow-up actions/risk mitigation plan:** A risk mitigation plan should be prepared to address priority areas and identified gaps and deficiencies. The plan should include actions such as enhancing controls or reducing inherent risks, depending on the inherent risk assessment.
3. **Regular review and updates:** REs are advised to review the IRA periodically, especially in response to changes in business activities, customer profiles, or emerging risks. REs can also internally determine the trigger events to initiate a review of IRA exercise apart from the periodic review process.
4. **Incorporation of proliferation financing (PF) risks:** A unique element to the RBI guidance is its inclusion of proliferation financing risks, which pose additional challenges. REs are encouraged to implement mechanisms to detect and prevent transactions that may facilitate the evasion of targeted financial sanctions, ensuring compliance with FATF and national regulations on PF.

A brief overview of various global guidance on AML/TF/PF risk assessment[3]

The need for RBI to issue a guidance note on internal risk assessment (IRA) stems from several key factors:

Financial action task force recommendations

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.

Basel committee on banking supervision guidelines

Banks must implement robust policies and processes, including strict customer due diligence (CDD) rules, to uphold high ethical standards and prevent misuse for criminal activities. Sound risk management involves identifying and analysing ML/FT risks within the bank and designing appropriate policies and procedures. Banks should conduct comprehensive risk assessments considering factors at the country, sectoral, bank, and business relationship levels to determine their risk profile and necessary mitigation measures.

3. a. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation- Financial Action Task Force (FATF) Recommendations, February 2016
b. Guidelines on Sound management of risks related to money laundering and financing of terrorism- Basel Committee on Banking Supervision (BCBS), January 2014 (rev. July 2020)
c. Terrorist Financing Risk Assessment Guidance, FATF, July 2019
d. Guidance on Proliferation Financing Risk Assessment and Mitigation, FATF, June 2021
e. Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines')- European Banking Authority (EBA), January 2024
f. The Wolfsberg Frequently Asked Questions (FAQs) on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption, 2015

FATF- TF risk assessment guidance-July 2019

A comprehensive assessment of terrorist financing (TF) risks requires the involvement of various key authorities, including intelligence and security agencies, law enforcement, financial intelligence units, customs, and regulatory bodies. The methodology for assessing TF risks should be flexible and tailored to the specific characteristics of each jurisdiction. It involves collecting a wide range of quantitative and qualitative information on the criminal environment, TF threats, vulnerabilities of specific sectors, and the jurisdiction's counter-terrorism financing (CFT) capacity.

Financing risk assessment and mitigation-June 2021

A PF risk assessment aims to identify, analyse, and mitigate PF risks through a systematic process involving both government and private sector stakeholders. This assessment should be comprehensive enough to inform national counter-proliferation strategies and ensure effective implementation of TFS. It involves compiling data on known threats, key sectors, and activities of designated individuals or entities. For private firms, relevant data includes customer due diligence information, transaction records, and threat analysis reports.

European banking authority guidelines

To comply with directive (EU) 2015/849, firms must assess the money laundering (ML) and terrorist financing (TF) risks they face due to their business's nature and complexity (business-wide risk assessment) and from individual business relationships or transactions (individual risk assessments). They should evaluate both inherent risks and the effectiveness of their controls and mitigation measures. The business-wide risk assessment should be tailored to the firm's specific profile, considering all relevant factors and risks, whether conducted internally or by an external party. When identifying ML/TF risks in business relationships or transactions, firms should consider customer profiles, geographical areas, products, services, transactions, and delivery channels.

Wolfsberg FAQs on risk assessments for money laundering, sanctions and bribery & corruption

The primary goal of a money laundering risk assessment is to enhance financial crime risk management by identifying the specific and general money laundering risks faced by a financial institution (FI), evaluating how these risks are mitigated by the institution's anti-money laundering (AML) controls, and determining the residual risk. The outcomes of such an assessment can be used to identify gaps in AML policies, make informed decisions about risk appetite and resource allocation, align AML compliance programs with risk profiles, develop risk mitigation strategies, inform senior management and regulators about key risks and control gaps, and ensure that resources and priorities are appropriately aligned with the institution's risks.

Conclusion

The guidance note is a welcome move from the RBI as it makes AML/TF risk assessment process more streamlined. It equips the financial institutions to manage not just today's risks, but also anticipate and mitigate future challenges in the ever-evolving landscape of financial crimes. Moreover, the adoption of a risk-based approach, detailed methodology for risk identification, and the inclusion of proliferation financing risks align Indian financial institutions with international standards.

KPMG in India contacts:

Akhilesh Tuteja
Head - Clients & Markets
E: atuteja@kpmg.com

Suveer Khanna
Partner and Head - Forensic Services
E: skhanna@kpmg.com

Sagrika Dani
Technical Director - Forensic Services
E: sagrikadani@kpmg.com

Anoop Sharma
Director - Forensic Services
E: anoopsharma@kpmg.com

kpmg.com/in

Access our latest insights
on KPMG Insights Edge

Follow us on:

kpmg.com/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.