INTERNAL RISK ASSESSMENT GUIDANCE FOR MONEY LAUNDERING/ TERRORIST FINANCING RISKS

10.10.2024

Contents

LIST OF ABBREVIATIONS

AML	Anti-Money Laundering
BCBS	Basel Committee on Banking Supervision
CDD	Customer Due Diligence
CFT	Countering Financing of Terrorism
CTR	Cash Transaction Report
DNFBP	Designated Non-Financial Businesses and Professions
EBA	European Banking Authority
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IRA	Internal Risk Assessment
KYC	Know Your Customer
LEA	Law Enforcement Agency
ML	Money Laundering
NBFCs	Non-Banking Financial Companies
NRA	National Risk Assessment
NPO	Non-Profit Organisation
PEP	Politically Exposed Person
PF	Proliferation Financing
RBA	Risk-Based Approach
RE	Regulated Entity
STR	Suspicious Transaction Report
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
UNSC	United Nations Security Council
WT	Wire Transfer

CHAPTER - 1

Foundation of the Internal Risk Assessment

1.1 INTRODUCTION

1.1.1 In an ever changing business environment and the increasing level of complexities in the banking and other financial products offered by banks and other regulated entities (REs), there is always a likely exposure to the elevated money laundering (ML)/ terrorist financing (TF)/ proliferation financing (PF) risks. The risks are further multiplied as use of emergent technologies and newer methods of payments enter the scene. The REs are, accordingly, required to have appropriate level of control/mitigating measures, so as to ensure that the elevated ML/TF risks do not result in the financial institution being misused for ML/TF, willingly or unwillingly and do not lead to loss of reputation and/or other financial losses for having allowed the suspicious transactions routed through the banking channels/ financial systems without timely reporting as per prescribed procedures and regulations.

1.1.2 REs are obligated to comply with the ML/TF/PF related legal provisions in terms of PML Act 2002, PML Rules 2005, WMD Act 2005, UAP Act 1967 and other Orders/ Directions of Government and its agencies under these Acts. Further, REs are obligated to comply with the relevant regulations under the above legal provisions vide Reserve Bank's Master Direction (MD) on KYC dated February 25, 2016 as amended from time to time. In terms of the section 5A of the MD on KYC, REs, *inter alia*, have to carry out 'ML and TF Risk Assessment' ('Internal Risk Assessment' or 'IRA') exercise periodically to identify, assess and take effective measures to mitigate their money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

1.1.3 Risk based approach (RBA) is an over-arching requirement as per Recommendation 1 of the FATF Recommendations and also underscored in the PML Rules and MD on KYC for management of ML/TF risks by REs. The RBA by REs allows them to adopt a more configurable set of measures in order to deploy their resources more effectively and apply preventive measures that are

commensurate with the ML/TF/PF risks posed by the customers, in order to focus their efforts in the most optimal way.

> *"Sound risk management requires the identification and analysis of ML/TF risks present within the bank and the design and effective implementation of policies and procedures that are commensurate with the identified risks. In conducting a comprehensive risk assessment to evaluate ML/TF risks, a bank should consider all the relevant inherent and residual risk factors at the country, sectoral, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied. The policies and procedures for CDD, customer acceptance, customer identification and monitoring of the business relationship and operations (product and service offered) will then have to take into account the risk assessment and the bank's resulting risk profile. A bank should have appropriate mechanisms to document and provide risk assessment information to competent authorities such as supervisors."*
>
> *– Excerpts from BCBS Guidelines on Sound management of risks related to money laundering and financing of terrorism.*

1.1.4 For sound management of risks related to ML and TF, BCBS has issued comprehensive guideline in January 2014 for banks, was last revised in July 2020 (https://www.bis.org/bcbs/publ/d505.htm). The guidelines not only prescribe the essential elements of sound ML/TF risk management, but also underpin the importance of RBA for identification, assessment and mitigation of ML/TF risks in the banks. Similarly, the FATF prescribes and requires the financial institutions to adequately apply ML/TF preventive measures commensurate with their risks and report the suspicious transactions. There are relevant guidance documents on risk assessments for ML/TF risks issued by EBA, World Bank, IMF, etc.

1.2 APPLICABILITY OF GUIDANCE

This guidance document is intended for all REs of the Reserve Bank (i.e., banks, NBFCs, Authorised Persons, Payment System Operators, etc.). In addition to supporting the RE's risk assessment and compliance efforts, the document also intends in helping to formulate the internally developed RBA of the respective REs by laying down certain

broad principles, methodology, etc. The senior management and employees of the REs engaged in their respective internal ML/TF risk assessment may refer to this document for this purpose.

1.3 KEY PRINCIPLES FOR AN INTERNAL RISK ASSESSEMENT (IRA) EXERCISE

1.3.1 The enterprise level risk assessment forms the bedrock of RBA. It enables the REs to understand how and to what extent, they are vulnerable to ML/TF/PF risks which help REs in determining the allocation of attention and AML/CFT resources necessary to mitigate that risk.

1.3.2 The following broad principles should be considered for carrying out an IRA exercise:

1.3.2.1 Dual-level IRA for ML/TF risks:

(a) Business Level IRA - The ML/TF/PF risk to which REs are exposed is a result of the specific business model, viz., nature and complexity of their business. IRA should be commensurate with the nature and size of REs' business.

Explanation: A simple risk assessment might suffice for REs of smaller size or REs offering less complex products/services which cater to only low-risk customers,. Whereas, in case, the size of operations is large, products and services offered are more complex or where RE offer services in various jurisdictions or its customer base is bigger or more diverse, a detailed and a sophisticated risk assessment process will be required.

(b) Individual Level IRA - The ML/TF risk to which REs are exposed is a result of entering into a business relationship with their customers or carrying out an occasional transaction for walk-in customers. When identifying ML/TF risks associated with a business relationship or occasional transaction, RE should consider relevant risk factors including who its customer is, the countries or geographical areas the RE operates in, the particular products, services and transactions the customer requires and the channels the RE uses to deliver these products/services/ transactions. The individual risk

assessment results in risk-categorisation of the customer into high, medium or low.

1.3.2.2 REs should use the IRA 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. Further, outcomes of the individual risk assessment should be factored in the business level IRA exercise so as to guide allocation of weights during the IRA exercise. For instance, customer level risk assessment may reveal that more of 'x' type of customers are opening accounts with the bank and if these are 'high risk' customers, then this should be factored in the IRA and appropriate (higher) weight should be given to the customer risk factor for correct identification of the risk. On the other hand, if more of 'y' type of customers are opening accounts with the bank and if these are low risk customers then risk weight may be adjusted accordingly in the IRA exercise. It may be useful to compare the risk-categorisation profile of clients in a RE and ML/TF/PF incidents for finetuning the exercise.

1.3.2.3 Each risk assessment level should consist of two distinct but related steps:

i. the identification of ML/TF risk factors; and
ii. the assessment of ML/TF risk and its impact.

1.3.2.4 In identifying and assessing the ML/TF risk to which they are exposed, REs should consider a range of ML/TF risk factors (key-risk factors) which may include:

(a) Inherent Risk Factors

i. The nature, scale, diversity and complexity of their business;
ii. Profile of the customers served;
iii. Type of on-boarding – Face-to-face or non-face-to-face;
iv. Type of customer – individual/ legal entity/ legal arrangement including trusts;
v. Products and services offered to customers, for example, cash-intensive products, non-face to face products, digital products, domestic and cross-border remittances, trade-based products, correspondent banking related services, etc.;

vi. Product/ service where transparency could be low in respect of beneficial ownership/ source of funds and wealth;
vii. Risks due to new technology products, payment methods, etc.;
viii. The volume and size of its transactions, considering the usual activity of the RE and the profile of its customers;

(b) Control Risk Types

i. Ability or lack thereof, to obtain necessary information in case of wire-transfers;
ii. The jurisdictions the bank is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organised crime, and/or deficient AML/CFT controls and are listed by FATF;
iii. The distribution channels such as ATMs, Business Correspondents, Mobile applications, branches, etc.;
iv. Outsourcing, third party reliance and dependence on unregulated intermediaries for provision of products/ services;
v. The internal audit and regulatory observations;
vi. Clientele where special relaxations have been provided in due diligence requirements;
vii. Pattern of collective de minimis transactions in different products.

Note 1. REs should gather sufficient information so that they can identify all relevant risk factors.. REs are expected to work out their own internal key factors for assessment while finalizing their internal guidelines. Some of the aforementioned risk-factors have been described in detail later in this guidance document. However, the REs may also monitor the key risk factors related to KYC and ML/TF on a periodic basis to evaluate a shift in trends of their ML/TF risk.

1.3.2.5 REs should use information obtained from all relevant internal and external sources for the IRA exercise. Internal sources include data/information from specific business relevant information from other related verticals of REs (such as fraud/cyber/IT risk management verticals), etc. Further, the internal

information should also include RE's own assessments of threats and vulnerabilities emanating from the respective business/operations as also future plans/strategies for business which will impinge on the ML/TF risks. As for external sources, the major elements may be the following:

i. National Risk Assessment (NRA) report of the Government of India;

ii. reports/public statements/press releases published by inter-governmental international organisations such as FATF, etc.;

iii. Guidance and advisories from Government authorities, FIU-INDIA, Reserve Bank, etc.;

iv. inputs from major national and international events/ market developments/ technology trends relevant to ML/TF risks;

v. research reports from accredited agencies, etc.;

vi. permitted Law Enforcement Agencies (LEA) databases and analytics;

vii. open-source intelligence such as from news articles, market inputs, etc., about products, customers, transactions, etc.

1.3.2.6 To properly understand the products/services and the associated ML/TF risks, IRA team may include officials, for instance, from the product/service owner department, internal audit function, compliance function, etc. A siloed approach wherein only the AML team is involved in the IRA exercise should be avoided.

1.3.2.7 REs may endeavor to adopt a data oriented objective approach to avert any kind of bias in the IRA exercise while quality of data inputs would need to be ensured so that the results are meaningful/useful. However, qualitative inputs and if necessary, expert judgements should also be used to ensure a comprehensive assessment of Type II errors. For instance, it may be desirable at times to interview product owners in other departments/verticals to understand the product and associated risks in depth.

1.3.2.8 Keeping in view the requirements under clause (b) of section 4 of MD on KYC, the IRA exercise may have a group-wide assessment which can aid in addressing the risks through a group-wide policy and programmes.

1.3.2.9 While addressing the uniqueness of ML/TF risks in the IRA exercise, wherever relevant, the linkages to related risks such as fraud risks including cyber fraud risks may be taken into account by the REs.

1.3.2.10 REs may consider the level of inherent risk, the relative quality of controls and risk mitigating factors while assessing the overall level of residual ML/TF risk associated with their business and with individual business relationships and / or occasional transactions.

1.3.2.11 Integrity of the critical processes in REs for ML/TF risk management such as CDD, Transaction Monitoring, Sanction Screening under Targeted Financial Sanctions (TFS), Alert generation/management, CTR/STR reporting, etc., needs to be ensured.

1.3.2.12 In respect of assessment of TF risks, some key distinctions with ML risks may need to be kept in view by REs. While under ML, the funds may emanate from illegal activities, funds employed for TF may come from both legitimate and criminal activities. The objective of TF, usually, is to facilitate acts of terrorism and ultimate beneficiary, generally, would be a person connected with terrorism. Though small-size/low-volume transaction may be non-material in ML risk, same may pose higher risk in case of TF.

1.3.2.13 The IRA exercise and the methodology used should be properly documented, maintained and communicated to relevant stakeholders within the RE and may be made available to competent authorities, if needed.

1.3.2.14 The IRA report, inter alia, should include the following to enable the stakeholders within the RE to have a comprehensive view of the outcomes of the report:

i. brief profile of the RE;
ii. executive summary;
iii. threats of ML/TF faced;
iv. inherent ML/TF risks and vulnerabilities assessed;
v. methodology applied for the assessment;
vi. ML/TF risk-factors assessed;

vii. controls applied;

viii. residual risk identified;

ix. outcomes;

x. mitigating measures proposed;

xi. enforcement actions taken by supervisors, LEAs, etc., during the last five years;

xii. observations and findings of internal audit regarding AML/CFT measures of the RE;

xiii. case studies or illustrations may be included, wherever appropriate.

Note 2. Wherever required, ranking of vulnerabilities, risks, mitigation measures, etc., may also be provided in the report to draw attention of the Top Management on high-priority issues.

1.3.2.15 The outcome of the IRA exercise should be put up to the Board or any committee of the Board to which power in this regard has been delegated. Sufficient additional information may be provided to them to understand and take a view on the findings.

1.3.2.16 REs should review the IRA periodically and, in any case when there in any change in business activities, or relevant new threats emerge. REs can, therefore, internally determine triggers to initiate a review of IRA exercise apart from the usual periodic review process. The trigger events could be, for example, introduction of a new product by the RE, expansion in new jurisdictions, NRA report shared by the Government, sectoral risks and vulnerabilities/ adverse observations shared by regulator, certain adverse observations/ findings of internal audit, change in profile of the RE, etc. REs should ensure that they have systems and controls in place to identify emerging ML/TF risks, assess these risks and, where appropriate, incorporate them into their risk assessment in a timely manner. The emerging risks could be identified through typologies report published by FATF, typologies shared by FIU-INDIA or the supervisor, alerts by LEAs, public statements of FATF, UNSC resolutions, the firm’s own knowledge and professional expertise, information

from industry bodies, information from FATF Mutual Evaluation reports of countries, information from credible and reliable sources.

1.3.2.17 An IRA which is not sufficiently granular, or which is not specific enough to reflect on the RE's functions and the risks to which it is exposed as a result of its activities, may not be able to meet the objectives of the exercise

CHAPTER - 2

Methodology and Quantification of ML/TF Risk Assessment and Control measures

2.1 METHODOLOGY

2.1.1 There are various ways in which an RE may decide to conduct its IRA exercise. One of the commonly used approaches internationally is the "conventional or standard methodology."[1] The first step of this approach is to identify the general and specific ML/TF risks ('Inherent Risks') that the RE faces, the second step involves determining how the RE can mitigate the risks identified in the first step with its AML/CFT programme controls ('Internal Controls') and third step involves establishing the residual risk that remains after applying the risk mitigants.

2.1.2 **Broad steps of this methodology are summarized as under:**

2.1.2.1 Define the inherent risk factors (RF) such as 'customer risk factor', 'geographic risk factor', 'products, services and transaction risk factor', 'delivery risk factor' etc. Further, define the sub-risk factors (SRF) under the RFs as applicable. For instance, under the 'customer risk factor', SRFs may be 'type of customer', 'complexity of customer's ownership', 'occupation of customer', 'PEP status', etc.

2.1.2.2 Collect the data on the RFs/SRFs.

2.1.2.3 Assign weights to the RFs/SRFs based on their contribution to the overall (enterprise-wide) ML/TF/PF risk.

2.1.2.4 Assign weight ('W_i') to the risk factor (RF_i) / sub-risk factor (SRF_i) based on its contribution in the ML/TF/PF risk posed by the concerned RF/SRF. This may

[1] The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption - https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf

be based on expert judgement and/or considering the data relating to it (please refer to paragraph 2.1.2.2 above).

For instance, for risk factor 'a' ('RF_a'), weight 'W_1' may be assigned to sub-risk factor 1 ('SRF_1'), weight 'W_2' may be assigned to sub-risk factor 2 ('SRF_2'), and so on. This would result in the final inherent risk ('IR') outcome for RF as:

$IR\_RF_a = W_1 * S\_SRF_1 + W_2 * S\_SRF_2 + \ldots$

Where:

i. IR_RFa is the "Inherent Risk for risk factor RF_a"

ii. W_i is the weight assigned to the sub-risk factor (SRF_i) based on its *contribution* in the ML/TF/PF risk posed by the concerned RF;

iii. S_SRF_i is the score assigned to sub-risk factor SRF_i, which may be based on the ML/TF/PF risk posed by it to the REs. For instance, if the RE takes a three-point scale, then score of 1 may be given in case of low-risk posed by the SRF, 2 in case of medium-risk and 3 in case of high-risk.

iv. $\sum W_i = 100\%$

(For further details on ii and iii above, please refer to paragraph 2.3 below)

2.1.2.5 The weighted inherent risk score (e.g., 'IR_RF_a' above) for each RF as calculated above, should be mapped to appropriate risk levels viz., 'High', 'Medium' and 'Low' to arrive at the 'inherent risk level'.

2.1.2.6 Identify and define the main control factors ('CFs') which help mitigate and control the inherent risk of the concerned RF/ SRF. For instance, for RF 'product and services', the CFs may be 'policies and procedure', 'product approval process', etc.

2.1.2.7 Assign weightage to each CF according to the relative contribution / importance it carries in mitigating and controlling the inherent risk of the particular RF. This may be based on expert judgement and/or considering the revenant data collected for this purpose by the RE.

For instance, for risk mitigation and control measures for RF 'product and services', the CF 'policies and procedure', may be given x% weight, 'product approval process' may be given y% weight and so on.

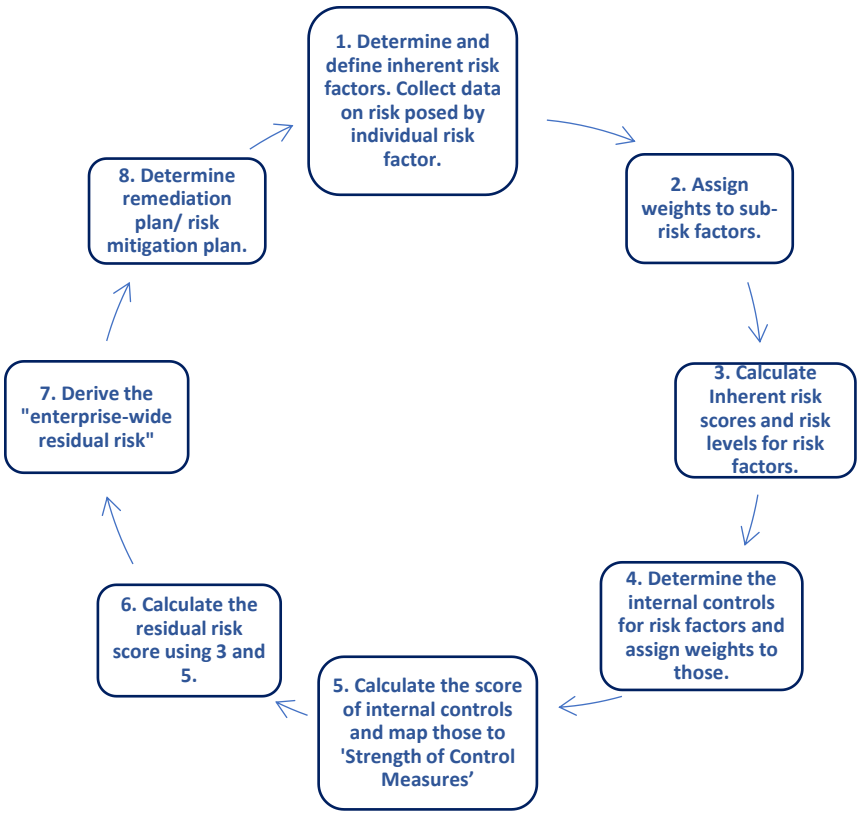
2.1.2.8 Similar to the scoring of the inherent risk factors as indicated at paragraph 2.1.2.4 above, derive the weighted score for the internal controls viz., the 'control effectiveness score' for that RF which should be mapped to the 'Strength of Control Measures' viz., 'Strong', 'Satisfactory' and 'Weak' for the Risk factor (considering a three-point scale).

2.1.2.9 Take the 'Inherent Risk Level' as derived in paragraph 2.1.2.4 above and apply the 'Strength of Control Measures' arrived at paragraph 2.1.2.8 above to arrive at the residual risk (RR) for each RF. For instance, residual risk RR_a may be arrived for RF_a. A residual risk matrix may be used for this purpose i.e., to arrive at RR_a. An illustrative residual risk matrix is provided below:

Inherent Risk → / **Strength of control measures** ↓	Low	Medium	High	
Strong	Low	Low	Medium	**Residual Risk**
Satisfactory	Low	Medium	High	
Weak	Medium	High	High	

2.1.2.10 The enterprise-wide residual risk may, thereafter, be derived using the weighted average of residual risks (RRs) of the RFs. Determine the remediation action plan or risk mitigation plan.

2.1.2.11 The graphical representation of the methodology is depicted as below-



Certain important aspects of the methodology are elaborated in detail in the following paragraphs:

2.2 RISK FACTORS

Following are certain risk factors which REs may consider in their IRA exercise. It may be noted that this is an indicative list and REs should invariably examine and define the risk factors that they may be exposed to.

2.2.1 Customer Risk Factors: When identifying the risk associated with their customers, including their customers' beneficial owners, REs should consider the risks related to:

i. Type of customer – individuals; legal entities such as companies; legal arrangements such as trusts; DNFBPs, NPOs, etc.;
ii. Complexity of customer's ownership and control structure;
iii. Occupation or profession or industry/business of the customer;
iv. PEP status as defined in regulatory directions;

v. Independent information sources for customer background – credible adverse media reports or other relevant sources of information about the customer.

2.2.2 Countries and Geographical Areas: When identifying the risk associated with countries and geographical areas, REs should consider the risks related to:

i. the jurisdictions with which the customer and beneficial owner is associated;
ii. the jurisdictions that are the customer's and beneficial owner's main places of business;
iii. the jurisdictions to which the customer and beneficial owner have relevant personal or business links, or financial or legal interests; and
iv. the jurisdictions in which RE operates.

2.2.3 Products, Services and Transactions Risk Factors: When identifying the risk associated with their products, services or transactions, REs should consider the risks related to:

i. the level of transparency or opaqueness of transactions in the product or service;
ii. the complexity of the product, service or transaction; and
iii. the value or size of the product, service or transaction.

2.2.4 Delivery Channel Risk Factors: When identifying the risk associated with the way in which the products or services are provided to the customers, REs should consider the risks related to:

i. the extent to which the business relationship is conducted on a non-face-to-face basis;
ii. an intermediary, such as use of business correspondent, payment aggregator, payment gateway, etc., which REs might use and the nature of their relationship with the REs; and
iii. the proven/observed vulnerability of channels likely to be compromised.

2.2.5 Other Risk Factors: REs should consider the risks related to:

i. Outcomes of sectoral risk assessment and NRA;
ii. Planned introduction of new products/services;

iii. Changes in the internal systems deployed for AML alerts;
iv. AML compliance employees turnover;
v. Enforcement actions by LEAs due to AML/CFT lapses; and
vi. Supervisory actions due to KYC/AML/CFT lapses.

2.3 ASSIGNING WEIGHTS TO THE RISK FACTORS AND SUB-RISK FACTORS

2.3.1 As mentioned in paragraph 2.1.1.4, REs may assign weight (W_i) to a sub-risk factor (SRFi) based on its contribution in the ML/TF/PF risk posed by the concerned RF. For instance, if the SRF 'complexity of customer's ownership/ownership structure' for the RF 'customer' is assessed to be contributing high ML/TF/PF risk for the RF 'customer', then a higher weight may be assigned to this SRF. Similarly, for assigning weights to RFs also, one RE may decide to place higher weight on customer risk factor (considering that it has a diverse set of customers) compared to the weight it places on the product. Another RE may decide to place more weight to product risk in case it has a lot of complex products to offer to its customer.

Within a risk-factor also, REs may assign different weights to the sub-risk factors. For instance, in case of customer risk factor, RE may assign weights to the sub-risk factors such as occupation of a customer, structure of the ownership, etc., differently.

2.3.2 It may be noted that the weight ('W') assigned to a SRF and the score ('S_SRF') assigned to that SRF need not be correlated necessarily. For instance, while a RE may assign a higher weight (W_i) to a SRF_i (e.g. – "complexity of customer's ownership/ownership structure" under the RF "customer") because it assesses that the contribution of ML/TF/PF risk due to this SRF_i to RF_a is generally high (as per internal and/or external sources), it may still assign a 'low-risk' score to this SRF_i (viz., S_SRF_i = '1' or 'low-risk') because only a fraction of its customer base has complex ownership structure. In such a case while 'W_i' may be high but 'S_SRF_i' may be low.

2.3.3 When assigning weights to the risk factors, REs should endeavor to ensure that

i. weight is not unduly influenced by only one factor ;

ii. economic or profit considerations do not influence the risk weights; and

iii. weight does not lead to a situation where it is impossible for any business relationship to be classified as high risk. There may also be situations which may actually present a high level of ML/TF risk, but which may not be appropriately reflected in the assigned risk weight. Such situations need to be identified by REs on case-to-case basis and REs should allow the risk scores calculated using the methodology to be overridden to a higher risk score. The rationale for the decision to over-ride such scores, however, should be documented appropriately.

iv. The views taken by regulator or LEA, for different violations/non-adherence to norms by the RE should also be weighed in.

2.3.4 Where a RE takes assistance from an external party/ vendor for conducting IRA or uses IT systems/ models to allocate overall risk scores, it should have clear understanding of how the system works and how it combines or weighs the risk factors to achieve an overall risk score. REs must satisfy themselves that the scores allocated reflect their own understanding of ML/TF risk and it should be possible to demonstrate this to the competent authority.

2.4 RISK CLASSIFICATION

2.4.1 REs should appropriately categorise the risks they have identified. Risk-categorisation should take place at various levels, for example, at the level of sub-risk factors such as occupation of a customer. The risk-score and risk weight of a sub-risk factor such as occupation of customers, will generate a weighted score at sub-risk factor level which will then contribute to the risk score to be derived at the risk factor level, for example, at the ‘customer risk factor’ level.

2.4.2 The risk-categorisation will depend on the nature and size of the RE’s business and the types of ML/TF risk the risk factor generates for the RE. Although REs generally categorise risk on a three-point scale of high, medium and low, other categorisations such as five-point scale are also possible.

2.4.3 Following their risk assessment and having considered both inherent risks and the mitigants applied, REs should categorise their business lines as well as business

relationships and occasional transactions according to the perceived level of ML/TF risk.

2.5 INTERNAL CONTROLS

2.5.1 Adequate internal controls are a prerequisite for the effective implementation of policies and processes to mitigate ML/TF risk. Post identification and assessment of inherent risks, as indicated above, internal controls need to be identified and evaluated to determine their effectiveness in controlling the overall risks. The internal controls as mentioned above shall include:

i. Governance and assurance function;
ii. Integrity of staff and compliance culture;
iii. Policies and procedures;
iv. KYC/ due diligence;
v. Monitoring and controls;
vi. Ongoing monitoring;
vii. AML Unit/ Team;
viii. Suspicious transaction reporting;
ix. Screening of sanctions lists such as sanctions lists pursuant to UNSC Resolutions 1267(1999), 1373(2001), etc., and freezing of accounts. Factors such as - effectiveness of the name matching in various combinations, frequency of screening, whether applicable to only account-based relationships or transactions also, etc., should be considered.
x. Independent testing/ model validations/ audit;
xi. Record keeping/retention;
xii. Training.

2.5.2 REs should determine and document not only the process of identifying the risk mitigants which are relevant for the IRA but also the process to evaluate the effectiveness of the identified risk mitigants. Effectiveness of the controls should be classified, such as highly effective, moderately effective, effective, less-effective, ineffective, etc. This is just an illustration and RE may decide to adopt any other scaling.

2.5.3 Similar to the inherent risk factors as mentioned above, each control factor may be assigned a weight based on its importance relative to other control factors. The weight and the score for a control factor will determine its contribution to the overall effectiveness of internal control or conversely, the 'overall effectiveness of internal controls' will be determined using the risk scores of individual controls and their weightage in the overall inherent control scheme.

2.6 RESIDUAL RISK

Residual risk is the risk that remains after internal controls are applied to the inherent risks. Post evaluation of 'overall inherent risk score' (e.g., 'medium') and the 'overall effectiveness of internal controls' (e.g., 'satisfactory'), the residual risk can be determined. The residual risk indicates whether the ML/TF risks within the RE are being managed adequately and effectively. REs may determine the scaling to be applied for residual risks. For example, residual risk may be scaled on High, Moderate and Low or alternatively as Low, Moderate-low, Moderate, Moderate-high and High. RE can adopt any scale which fits its IRA. However, each score in a scale such as high, medium or low on a three-point scale, should be defined for the purpose of classifying a residual risk in that scale. For instance, low residual risk may be defined as, 'the overall inherent risk, based on the risk factors is low/ moderate and the mitigating internal controls are effective to manage this inherent risk'. REs may prepare a residual risk matrix for this purpose with inherent risk scores as rows/columns and control scores as columns/rows, as per their preference. In order to improve its residual ML/TF risk, RE should either reduce the inherent ML/TF risk or strengthen the AML/CFT controls and a strong control environment can always lower the residual ML risk vis-à-vis a low control environment.

CHAPTER - 3

Follow-up actions and incorporation of Proliferation Financing Risk in IRA

3.1 COMMUNICATION OF IRA RESULTS

REs should communicate the IRA results to Board or Committee of the Board as required under the MD on KYC. Further, the results should also be communicated to other relevant stakeholders within the RE and business verticals, as appropriate, for them to act upon the findings of the IRA exercise in an effective manner.

3.2 FOLLOW-UP ACTIONS/ RISK MITIGATION PLAN

Following the completion of IRA exercise, RE should act upon the priority areas/gaps/deficiencies identified. Residual risk has to be seen in the context of risk appetite/ tolerance of the RE given the legal/regulatory obligations related to ML/TF management as also specific strategic/tactical measures proposed/implemented by management. A risk-mitigation plan should be prepared to reduce the residual risks going forward – by reducing inherent risks, enhancing controls, etc. Utmost attention and support from the senior management and other relevant stakeholders within RE must be provided. An RE may decide, based on the gravity of the issues identified, to conduct next review of the IRA even prior to the set periodicity.

3.3 INCORPORATION OF PROLIFERATION FINANCING RISK IN IRA

3.3.1 The proliferation financing risks emanates broadly from (i) risk of a potential breach or non-implementation of targeted financial sanctions, and (ii) risk of evasion of targeted financial sanctions.

3.3.2 In terms of clause (c) of section 4 of MD on KYC, REs should have an adequate policy framework seeking to ensure compliance with all legal and regulatory instructions for providing a bulwark against threats arising from ML/TF/PF and other related risks. While ensuring compliance of the legal/regulatory requirements as above, REs may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better. Accordingly, REs while ensuring compliance with section 12A of WMD Act 2005 and associated Government Orders, may carry out an appropriate PF risk assessment for their institution and suitably incorporate the same in internal ML/TF

risk assessment (IRA) as also ensure suitable mitigation measures. Further guidance may be taken in this regard from the 'Guidance on Proliferation Financing Risk Assessment and Mitigation'[2] dated June 2021 of FATF.

[2] https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf

REFERENCES

(a) Basel Committee on Banking Supervision (BCBS) Guidelines 'Sound management of risks related to money laundering and financing of terrorism'.
https://www.bis.org/bcbs/publ/d505.pdf

(b) International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (The FATF Recommendations):
https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

(c) European Banking Authority (EBA) 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') under Articles 17 and 18(4) of Directive (EU) 2015/849:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

(d) The Wolfsberg Frequently Asked Questions (FAQs) on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption:
https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf

(e) FATF - Terrorist Financing Risk Assessment Guidance - July 2019
https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Terrorist-Financing-Risk-Assessment-Guidance.pdf

(f) Guidance on Proliferation Financing Risk Assessment and Mitigation – June 2021
https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf