Guidance for a risk-based approach for remittance services providers

304 E 45th Street,
New York, United States

Email: info@uncdf.org

ACKNOWLEDGMENTS

On behalf of the migrant women and men originating from, and receiving remittances in, their wider communities in least developed countries, the UNCDF Migrant Money programme team would like to thank the many partners and collaborators who are contributing to our efforts to advance the work on addressing challenges and frictions facing remittance flows. This appreciation is not their endorsement of this paper and is extended to many stakeholders, including programme staff, implementation partners, knowledge leaders, expert influencers, wider global advocates and advocacy organizations, United Nations colleagues, collaborators in the wider fields of international and development finance and in the financial and remittance industries, research participants, regulatory and policymaking leaders, and many other individual or organizational stakeholders.

The drafting of this guidance for a Risk-Based Approach for Remittance Services was led by Mercy W Buku, Legal and Risk Management Consultant – Digital Financial Services. Invaluable input and contributions were also made by Albert Mkenda, Bisamaza Mukankunga, Doreen Ahimbisibwe, Deepali Fernandes, and Paloma Monroy. Additionally, Djeinaba Kane, Jacqueline Jumah, and Tewodros Besrat from AfricaNenda, along with Amadou Cisse and Lydia Kinyanjui from the African Institute of Remittances (AIR), offered invaluable insights. Officials from the Central Banks of the ECCAS and IGAD Member States also played a crucial role in this process. Amil Aneja and Eliamringi Mandari provided overall guidance and coordination.

The authors would also like to thank John Powell and Justine De Smet for editorial and design support.

The UNCDF Migrant Money programme has been made possible by the generous funding support from the Swiss Agency for Development and Cooperation and from the Swedish International Development Cooperation Agency. This work is a product of the staff of the UNCDF with external contributions. The findings, interpretations, and conclusions expressed do not necessarily reflect the views of the UNCDF, its executive board and donors, or the governments they represent. UNCDF does not guarantee the accuracy of the data included in this work.

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

AML	anti-money laundering
AML/CFT	anti-money laundering/combating financing of terrorism
ATM	automated teller machine
CDD	customer due diligence
CFT	combatting the financing of terrorism
ECCAS	Economic Community of Central African States
EDD	enhanced due diligence
e-KYC	electronic know your customer
FATF	Financial Action Task Force
FIU	financial intelligence unit
ID	identification
IGAD	intergovernmental authority on development
KYC	know your customer
ML	money laundering
ML/TF	money laundering/terrorist financing
MVTS	money or value transfer services
NPPS	new payment products and services
PEP	politically exposed person(s)
RBA	risk-based approach
RSP	remittance service provider
STR	suspicious transaction report
SDD	simplified due diligence
TF	terrorism financing
UN	United Nations
UNCDF	United Nations Capital Development Fund

EXECUTIVE SUMMARY

UNCDF's Migration and Remittances for Development Programme, or the Programme, aims to support sustainable development by making remittances more accessible and affordable while helping build resilience for migrants and their families. For remittance service providers (RSPs), the Programme seeks to build the capacity to understand the financial needs and preferences of migrants and their families and to design and deliver responsive products accordingly.

Under the Financial Action Task Force (FATF) Recommendations,[1] countries are required to put in place effective risk management frameworks as well as guidance for RSPs in compliance with AML/CFT legislation[2] without imposing an unwarranted burden on lower-risk RSPs and restricting access to financial services to those seeking to use remittance services for their financial needs.

This guidance aims to assist regulators in implementing enabling regulatory frameworks for remittance services, as advocated by the FATF Recommendations. It comprises best practices and processes to guide RSPs on compliance with the FATF recommendations and national AML/CFT legislation using RBA.[3]

[1] The Financial Action Task Force is the global standard setting body for AML/CFT Compliance. The FATF has developed globally accepted standards for combatting money laundering, terrorist and proliferation financing known as the FATF recommendations.

[2] This obligation extends to proliferation financing under Recommendation 7.

[3] The risk assessment measures set out in this guidance may also be adopted as a preventive measure for proliferation financing, as required under FATF Recommendation 7, where appropriate.

PART I – INTRODUCTION

Digitally enabled remittance services have increasingly become the most efficient method of making and receiving remittances. Various players are now using web- and mobile-based applications to allow remittances.

Remittance services can be important channels for driving financial inclusion. Mobile money remittances, for example, are now contributing to financial inclusion, particularly in Sub-Saharan Africa and South-East Asia — particularly among women — as a driver of account ownership and usage via mobile payments, savings, and borrowing.[4]

However, Remittance services are potentially at risk of being misused for money laundering and financing terrorism activities. The speed with which a remittance transaction takes place means that these platforms are vulnerable to abuse by those wishing to use them for money laundering and terrorism financing.

Under the FATF recommendations, RSPs must have robust AML/CFT programmes to facilitate compliance with their AML/CFT obligations. However, the FATF recognizes that applying an overly cautious approach to AML/CFT safeguards could unintentionally exclude legitimate businesses and consumers from the financial system, compelling them to use services not subject to regulatory and supervisory supervision.[5]

Mitigation measures for AML/CFT should be balanced to not impede access to formal financial services for the financially excluded and unbanked. As a result, the FATF opposes wholesale termination or restriction of business agreements and encourages the RBA to provide financial services.[6]

PURPOSE OF THIS GUIDANCE

These guidelines are intended to guide RSPs in dealing with money laundering and terrorism financing risks by adopting an RBA. RSPs may use the guidelines as a template for establishing internal controls and programmes for managing money laundering and terrorism financing risks in their business operations.

Regulators can also draw on this guidance to facilitate the implementation of enabling regulatory frameworks for remittance services by adopting an RBA as recommended by the FATF Recommendations.

[4] Global Findex database (2021).

[5] FATF Guidance on AML/CFT measures and financial inclusion, with a supplement on customer due diligence (fatf-gafi.org)

[6] FATF clarifies risk-based approach: case-by-case, not wholesale de-risking (fatf-gafi.org).

APPLICABILITY

This guidance applies to the following:

1. Non-bank RSPs and their agents.
2. Money or value transfer service providers, including mobile money and virtual assets service providers.
3. Registered hawala money transfer agents.

INTERPRETATION

In these Guidelines, except where the context otherwise requires,

Customer refers to the user of an RSP's services. Such a customer may be a legal (corporate) entity or a natural (individual) person.

Customer due diligence, or CDD, is the process of obtaining and verifying prescribed information to properly identify customers.

Financial inclusion means that individuals and businesses have access to useful and affordable financial products and services, delivered responsibly and sustainably, that meet their needs, e.g., transactions, payments, savings, credit, pension, insurance, etc. Access to a transaction account is a first step toward broader financial inclusion since a transaction account enables people to store money and send and receive payments.[7]

New payment products and services refer to prepaid cards, mobile payments, Internet-based payment services, and virtual asset services within the FATF guidance on the RBA for prepaid cards, mobile payments, internet-based payment services,[8] and virtual assets and virtual asset service providers.[9]

Remittance services, in the context of these guidelines, are cross-border financial services through which cash, cheques, other monetary instruments or stored value are received and a corresponding sum in cash or other monetary instruments is paid to a designated recipient via a communication, message, or transfer or through a clearing network or remittance hub. Remittance services are also known as money or value transfer services (MVTS).

A remittance service provider or RSP is an individual, non-bank business or organization that accepts instructions from customers to transfer cash, cheques, other monetary instruments or stored value to a designated recipient. Remittance service providers are also referred to as money transfer businesses.

A risk-based approach or RBA refers to identifying, assessing and understanding ML/TF risks facing RSPs and applying proportionate measures to mitigate these risks effectively and efficiently.

---

[7] https://www.cgap.org/research/publication/achieving-sustainable-development-goals.

[8] FATF RBA-NPPS-2013.html.

[9] Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (fatf-gafi.org)

VULNERABILITIES OF RSPS TO MONEY LAUNDERING AND TERRORIST FINANCING ACTIVITY

Remittance Services are vulnerable to various risk factors, which make them a target for exploitation by those seeking to use them for money laundering and terrorism financing. These factors are provided below:

1. **Speed, portability and anonymous nature:** The speed and portability of remittance channels make them attractive to criminals as conduits for money laundering. The anonymous nature of some remittance services means that money launderers can engage third parties to conduct transactions on their behalf and send or receive money via remittance services to protect the launderers' identity.

2. **Complex nature:** Technological advances in digital financial services have created a complex domestic and cross-border remittance ecosystem, creating challenges in supervising online money remittance services and making it easier for criminals to circumvent identity verification processes.

3. **New payment products and services:** Certain new payment products,[10] such as prepaid cards, can be used to send and receive money and to withdraw cash from ATMs with funds loaded anonymously over the Internet, e.g., through non-bank remittance apps. Fraudsters can also steal and use debit and credit cards to transfer funds through legitimate RSPs. These cards can also be used via open-loop remittance systems to transfer money worldwide, pay for goods and services, or withdraw cash without face-to-face transaction requirements. Other remittance channels which can be used as conduits for money laundering are mobile payment and virtual currency platforms, either directly or through linkages to RSP platforms through partnership arrangements.

4. **Regulatory Risk:** RSP supervision varies according to the jurisdiction, and money launderers may seek to exploit that disparity by moving illegal funds using cross-border remittance services. The lack of communication between supervisory authorities in different countries may make it difficult to track such remittances.

5. **Compliance Risks:** The speed and portability of remittance services require RSPs to put in place sophisticated automated real-time transaction monitoring systems to enable them to detect and monitor suspicious money laundering activities. These systems are expensive and require heavy capital expenditure, and not all RSPs can afford them, particularly non-bank RSPs. In recognition of this risk, RSPs are designated reporting entities under the FATF recommendations.[11]

[10] As defined in the FATF Guidance for a Risk-Based Approach: prepaid cards, mobile payments and Internet-based payment services.

[11] Examples of circumstances where RSPs may be subject to money laundering risks providing remittance services to their customers, are outlined in the UNCDF AML/CFT Guidance for RSPs.

PART II: CUSTOMER DUE DILIGENCE MEASURES FOR REMITTANCES

This section covers the general requirements for customer due diligence measures for remittances.

AML/CFT PROGRAMME

Under FATF Recommendation 18, designated reporting institutions must have AML compliance programmes with adequate systems and procedures to comply with AML/CFT obligations.[12]

An effective AML programme for RSPs will comprise policies and procedures incorporating the following checks:

a. Due diligence for customers, agents, and business partners
b. Transaction monitoring
c. Sanction screening
d. Suspicious activity reporting
e. Training and awareness for staff, agents, third-party partners, and customers
f. Risk assessments for customers and products
g. Agent management and compliance monitoring
h. Complaint recourse channels
i. Technical controls
j. Transactional controls for international money transfers and cross-border transfers
k. Provision of information for ML/TF investigations and law enforcement

CUSTOMER DUE DILIGENCE MEASURES FOR REMITTANCES

1. Under FATF Recommendation 10, RSPs are required to undertake CDD measures:
    a. when establishing business relations or carrying out occasional or one-off transactions;
    b. for transactions above the designated thresholds ranging from 10,000 to 15,000 US dollars/euros, depending on the jurisdiction;[13]
    c. when sending wire transfers as set out under section 2.4 below;
    d. where money laundering and/or terrorist financing are suspected; or
    e. where the RSP has doubts concerning the veracity or adequacy of previously obtained customer identification data.

2. RSPs should implement effective CDD to obtain and verify the requisite details to properly identify new customers. These requirements should extend to customers, agents, and business partners. The requisite details may differ from one jurisdiction to another as set out in their AML/CFT legislation.

[12] Refer to the UNCDF AML/CFT Risk Management Guidance for detailed AML/CFT processes for RSPs.

[13] FATF recommendations 10 and 22 prescribe a threshold of 15,000 US dollars/euros for occasional transactions, however many jurisdictions impose a lower threshold of $10,000 which is also applicable for reporting purposes.

3. These procedures should require RSPs to take reasonable measures to ascertain the true identity of all persons seeking to use their services, whether or not the services are offered over the counter or through established accounts. Such reasonable measures may include the following:
   a. Identifying customers and verifying their identity using reliable, independent source documents, data, or information.
   b. Identifying the beneficial owner and taking reasonable measures to verify the beneficial owner's identity, such that the RSP is satisfied that it knows the beneficial owner. For legal persons and arrangements, this should include RSPs understanding the customer's ownership and control structure.
   c. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
   d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout that relationship to ensure that the transactions are consistent with the RSP's knowledge of the customer, their business, and risk profile, including, where necessary, the source of funds.

4. Under FATF Recommendation 16, the following information should be collected from customers using the RSP's services for wire transfers:
   a. Accurate originator information, including the following:
      - The name of the originator
      - The originator's account number for the account used to process the transaction
      - The originator's address
      - National identity number or passport number
      - Date and place of birth
   b. Accurate beneficiary information, including the following:
      - The name of the beneficiary
      - The beneficiary's account number for the account used to process the transaction
      - A unique transaction reference number to enable tracing of the transaction if no account number is available

5. The information collected should be kept with the wire transfer or related message throughout the payment chain.

6. Where an RSP establishes customer accounts, it must maintain no anonymous accounts or accounts under fictitious names. All transactions must be properly verified for RSPs offering their services over the counter or through web-based or mobile applications.

7. Where it becomes apparent to the RSP that a customer with an account or person seeking to undertake a single transaction in the case of over-the-counter services is a sanctioned person, it must take steps to cease the business relationship with that person.

PART III: RISK-BASED APPROACH FOR REMITTANCE SERVICES

This section covers measures for applying a risk-based approach in remittance services.

FATF AND THE RISK-BASED APPROACH

This guidance is based on the Financial Action Task Force (FATF) recommendations,[14] internationally accepted guidelines issued by the FATF. The FATF is the Global standard-setting body for AML compliance. Countries should also refer to the provisions of their relevant AML/CFT legislation when developing RBA Guidance for the remittances sector. The RBA is heavily shaped by the following FATF Recommendations on AML/CFT Controls:

1. Under FATF Recommendation 1, countries must comply with FATF Recommendations in providing financial services to ensure that these services are not being abused for money laundering/terrorist financing and other criminal activities. In particular, countries must ensure that they have comprehensive anti-money laundering legislation that includes proper CDD measures for opening accounts that enable the identification of financial service users and permit the monitoring of ongoing customer connections. Countries must identify, assess, and understand the risks of money laundering and terrorist financing for different market segments, intermediaries, and products on an ongoing basis and employ a risk-based approach to take action and invest resources to mitigate these risks.[15] This requirement extends to supervisors or other authorities who are required to assess specific risks relevant to their functions. Equally, RSPs are required under Recommendation 1 to understand, identify and assess the ML/TF risks relevant to their activities. As stipulated in the FATF Recommendations 2012, the RBA is a necessary step.

2. The FATF Recommendations criminalize the offence of money laundering and terrorist financing and comprise various measures to prevent money laundering and terrorist financing as follows:
    i. KYC and CDD both at entry level and in ongoing customer relationships (including establishing beneficial owners for corporate clients)
    ii. Transaction monitoring to detect suspicious activity
    iii. Watch list screening against FATF-recommended sanctions list, e.g., those issued by the United Nations, European Union, His Majesty's Treasury (United Kingdom), and the US Office of Foreign Assets Control (OFAC), to detect possible terrorism financing activity
    iv. Suspicious activity reporting (internal and regulatory)
    v. Staff training on AML awareness
    vi. Record-keeping
    vii. Sanctions and penalties for non-compliance

[14] FATF recommendations 2012, updated March 2022.

[15] FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures (fatf-gafi.org)

3. With specific reference to RSPs, FATF Recommendation 14 on money or value transfer services requires countries to take appropriate measures to ensure that natural or legal persons that provide money or value transfer services are licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. This requirement extends to virtual asset providers under Recommendation 15.

4. The FATF has issued guidance notes on the RBA applicable to remittance services as follows:
   - FATF High-Level Principles on the Risk-Based Approach: FATF High-Level Principles and Procedures on the Risk-Based Approach.pdf
   - Guidance for a Risk-Based Approach for Money or Value Transfer Services: RBA-Money-Value-Transfer-Services.pdf
   - FATF Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services: FATF RBA-NPPS-2013.html
   - FATF Guidance - RBA Virtual Currencies FATF guidance-rba-virtual-currencies.html

RISK-BASED COMPLIANCE PROGRAMME FOR REMITTANCES

1. RSPs must understand, identify, and assess the ML/TF risks relevant to their activities and employ an RBA to mitigate these risks.

2. A risk-based AML/CFT compliance programme for RSPs should be tailored to manage risks arising from the services provided by the RSP and include the following measures:[16]
   a. Risk-based CDD policies, procedures and processes that identify and verify the information required to onboard customers and the action to be taken if such information is unavailable, including simplified CDD measures and procedures for entering into customer relations before an identity is established, in appropriate cases.
   b. Documentation of the risk assessment and risk appetite, specific to the type of business and customers, with appropriate parameters for risk categorization.
   c. Risk-based controls and measures for higher-risk and lower-risk customers.
   d. Ongoing monitoring of customer information and transactions against their profiles. Such monitoring will detect suspicious activity and screen for terrorist financing and PEP activity.
   e. Risk-assessing the impact of new products and business practices (or new technology on old products) before the launch of specific products/services with appropriate controls, including new payment products (mobile money and other digital financial services virtual assets service providers).
   f. Measures to identify high-risk operations (products, services, delivery channels, customers, and geographic locations).
   g. Regularly updating the RSP's risk profile.

[16] Also refer to the UNCDF AML/CFT Risk Management Guidance for other AML/CFT compliance measures that RSPs are expected to put in place.

3. During the inspection visit, RSPs should share their risk identification, monitoring and mitigation frameworks with the regulator to demonstrate their capacity to undertake appropriate ML/TF risk management.

4. The RBA is obligatory and must be taken by regulated RSPs to target AML resources proportionately, especially in areas of business where the risk of money laundering is high.

5. The RBA, however, does **NOT** apply to wire transfers due to the requirement to identify the originator and the beneficiary of a transaction under Recommendation 14.

THE RISK ASSESSMENT PROCESS

Under the FATF Guidance Note for Money or Value Transfer Services, institutions must conduct a risk assessment at the beginning of a customer relationship to identify potential risks that may create opportunities for ML/TF. This may also include carrying out the risk profiling of customers to categorize them as high, low, and medium risk for the documentation required. This, in turn, will determine the appropriate level of identification, verification, monitoring and additional customer information needs.

a. RSPs should take steps to identify and assess their ML/TF risks (appropriate to the nature and size of the business) and have policies, controls, and procedures to manage and mitigate such risks.

b. In the context of RSPs, institutions must **identify high-risk customers, products, and services, including delivery channels and geographical locations.** High-risk areas should be subject to enhanced procedures like CDD checks and transaction monitoring. It also follows that in instances where risks are low, simplified, or reduced controls may be applied.[17]

c. ML/TF risks are identified and categorized as high/medium/low according to the risk's severity, likelihood, and impact, using the criteria set out to assess the risk of customers and products.

d. Preventive mitigatory controls are assigned as appropriate, including EDD for high-risk transactions/customers, transaction monitoring, transaction limits, etc.

e. When carrying out the risk assessment, RSPs should consider the following factors:[18]
   - The nature, scale, diversity and complexity of their business and their target markets
   - The proportion of customers already identified as high-risk
   - The jurisdictions the RSP provider is operating in or otherwise exposed to, either through its activities or the activities of customers, especially in jurisdictions with greater vulnerability due to contextual and various risk factors such as the prevalence of crime, corruption, financing of terrorism,

[17] Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing ; FATF Guidance -National_ML_TF_Risk_Assessment.pdf | FATF AML and CFT measures and financial inclusion.

[18] Guidance for a Risk-Based Approach for Money or Value Transfer Services (fatf-gafi.org)

as well as the general level and quality of governance, law enforcement, AML/CFT regulation and supervision, including those listed by FATF

- The distribution channels, including the extent to which the RSP deals directly with the customer and the extent to which it relies on third parties to conduct CDD, the complexity of the payment chain and the settlement systems used between operators in the payment chain, the use of technology and the extent to which agent networks are used
- The internal audit and regulatory findings
- The volume and size of its transactions, considering the usual activity of the MVTS provider and the profile of its customers

IDENTIFICATION OF RISK FACTORS

As part of the risk assessment process, RSPs should identify and categorize risk factors applicable to remittances. These risk factors are made up of threats which may make the RSP vulnerable to ML/TF. Identifying and categorizing risk factors enables ML/TF risks to be assessed as high, medium, or low, depending on their potential impact on the business and existing mitigatory measures. Applicable risk factors for remittance services are set out below.

a. Geographic or country risk
   - *Indicator*: Dealings with entities or persons from risky jurisdictions, countries with porous borders, endemic corruption, lack of political goodwill and poor legislative frameworks to curb ML/TF and other financial crimes, and political instability in the neighbouring countries.

b. Financial services or product risk
   - *Indicator*: The prevalence of multiple financial services that criminals can exploit as channels for ML/TF, the proliferation of new products and fintechs arising from financial inclusion initiatives such as mobile money and other digital financial services whose speed, portability, and anonymity, offer a cheap and reliable channel for money laundering and terrorist financing, the presence of informal economies where cash is the preferred mode of payment.

c. Financial exclusion/customer risk
   - *Indicator*: RSPs in countries with largely unbanked, illiterate rural populations, underdeveloped CDD measures, inadequate CDD regulations and lack of national identification regimes will experience challenges in verifying customers' identity, which can create opportunities for identity theft and fraud.

d. Institutional and third-party risk
   - Indicator: The kind and type of business a country or institution conducts can provide chances for ML/TF, for example, when such entities have insufficient policies and processes for procuring and onboarding third-party partners such as suppliers, including tendering.

e. Agent or channel risk

- *Indicator*: Compliance monitoring and enforcement challenges may arise due to large government branch networks and remote locations, failure to carry out appropriate due diligence, e.g., on customers, suppliers and staff, and non-compliance with AML/CFT regulations, e.g., on KYC/CDD, transaction monitoring and sanction screening, and record-keeping.

f. System and delivery risks

- *Indicator*: Inadequate systemic controls, lack of appropriate transaction monitoring and investigative tools, and inadequate record-keeping processes can create fraud opportunities. Delivery of financial services through automated non-face-to-face channels and using third parties by regulated entities as part of the service delivery chain facilitates anonymity and makes transactions hard to track.

A sample Risk Rating Matrix and Case Study based on these indicators is appended hereto under Appendix A and B, respectively.

RISK PROFILING OF CUSTOMERS AND BUSINESS SEGMENTS

a. Risk Profiling of customers and business segments is an essential part of the risk assessment processes as it enables customers and business segments to be categorized according to their risk rating and adopt appropriate mitigatory measures to deal with the risk.

b. A comprehensive risk profile may only emerge once a customer transacts through an account. Therefore, monitoring transactions to obtain a clear view of 'normal' customer activity will be an important part of ongoing risk management.

c. Once the risk level has been assessed, appropriate mitigatory measures can be implemented depending on the customer's risk profile. For example, simple due diligence may be allowed for low-risk customers, with enhanced due diligence measures for customers assessed as high-risk. However, having a lower risk of money laundering and/or terrorist financing risk for identification and verification purposes does not automatically mean the same customer will be low risk for all types of products and CDD measures, particularly for ongoing monitoring of transactions.

OVERALL RISK ASSESSMENT

Once the risks have been analysed, they will be transferred to a 'heat map' to identify the overall money laundering risk. The heat map combines the outcome of the overall threat analysis with the overall vulnerability.

*A sample heat map is set out in **Figure 1** below. A sample risk assessment template for assessing the risks and proposed mitigatory measures is to be found in Appendix A.*

Figure 1: Overall money laundering risk as a combination of threat and vulnerability

OVERALL THREAT						
	H	M	M	MH	H	H
	MH	M	M	MH	MH	H
	M	ML	M	M	MH	MH
	ML	ML	ML	M	M	M
	L	L	ML	ML	M	M
		L	ML	M	MH	H
	OVERALL VULNERABILITY					

Source: World Bank National ML/TF Risk Assessment Tool- Module 1[19]

SIMPLIFIED DUE DILIGENCE UNDER THE RISK-BASED APPROACH

a. Concerning CDD, the risk-based approach affords RSPs the flexibility to adopt simplified CDD in proven low-risk scenarios.

b. The FATF Guidance on a risk-based approach[20] permits exemptions from AML/CFT obligations where simplified CDD can be applied in situations where there is proven low risk of money laundering and terrorist financing, for example, in limited and justified circumstances (for a particular RSP or activity) or de minimis situations when a natural or legal person carries out a financial activity on an occasional or very limited basis (having regard to quantitative and absolute criteria), relative to its other, primary business activities.

c. The FATF guidance also offers flexibility in applying FATF recommendations to ensure that certain vulnerable groups (e.g., low-income recipients, migrants, women and those assessed as low-risk) are not unreasonably excluded from accessing financial services.

d. Full or enhanced CDD is, however, compulsory where the risks are higher, e.g., for corporate entities, customers from high-risk countries, PEPs, customers carrying out high-volume transactions, etc.

e. FATF guidance specifically excludes wire transfers from the scope of the RBA.

[19] World Bank Risk Assessment Support for ML/TF.

[20] FATF Guidance on a Risk-Based Approach for Money or Value Transfer Services Guidance for a Risk-Based Approach for Money or Value Transfer Services (fatf-gafi.org) Also see FATF Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services. (Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services (fatf-gafi.org)

RECOMMENDED MEASURES UNDER THE RISK-BASED APPROACH

As noted above, the RBA may be extended to documentary requirements for CDD, business segments and products.

CUSTOMER DUE DILIGENCE DOCUMENTATION

Where standard identification requirements (for documentation or digital records) may not be readily available, RSPs must determine appropriate systems to handle these situations. The following are recommended CDD measures that RSPs can implement to facilitate access to remittance services in low-risk situations using the RBA.

RSPs should, however, check to confirm that these measures have regulatory approval or are otherwise allowed under the relevant AML/CFT regulations, which include the following:

a. Acceptance of other types of evidence of identities such as employment cards, student cards, birth certificates, driver's licenses, refugee cards (including status or residency permits for migrants) or other government-approved photo IDs for onboarding purposes.
b. Acceptance of letters or statements from an appropriate 'person of standing', e.g., a chief, head teacher of local administration officer, as proof of residence, and supporting letters from community leaders in refugee camps.
c. Acceptance of temporary documentation applicable to displaced persons or refugees, such as residency status permits, proof of registration or waiting slips.[21]
d. Delaying the implementation of CDD measures, for example, allowing the limited operation of accounts until full documentation is received.
e. Where SDD is allowed under regulation, the introduction of low threshold-based CDD for money remittances so as not to impose unreasonable identification requirements on those who may not have such documents.
f. Introduction of biometric registration for onboarding customers.[22]

[21] Registration processes for forcibly displaced people vary across countries, hence temporary documentation will be defined appropriately in the relevant Refugee legislation.

[22] This is relevant in countries where biometric registration supports simplified diligence as an alternative to traditional methods of identification and have a robust and secure digital identity infrastructure that can support the financial sector. Biometric information enables the storage of information which can be used to identify and verify customers at RSPs. It also fosters financial inclusion as eliminates the production of physical ID documents for financial transactions.

Country Examples of Simplified Due Diligence Measures[23]

1. **Kenya and Tanzania** have implemented measures for tiered KYC thresholds for the Mshwari and Mpawa digital banking savings and credit products, which are pegged to the M-pesa mobile money transfer service. The thresholds are based on the amount saved, with enhanced KYC measures, such as submitting copies of identification required for amounts over $2,500.

2. **Mexico** has approved a simplified due diligence structure for opening accounts pegged to low transactional volumes, for example, no physical identification card copies are required for accounts with transactions of less than $1,150 per month.

3. **The Philippines** have temporarily relaxed identification requirements following a natural disaster, with specific controls on transaction limits and relaxed documentation requirements to facilitate payments to persons displaced by Typhoon Haiyan in November 2013.

4. Chile allows deposit accounts to be linked to tax numbers for low-income persons in Chile.

5. **Fiji** allows people to open accounts with an appropriate referee letter and a birth certificate in place of a formal ID. Suitable referees are widely categorized.

PRODUCTS/BUSINESS SEGMENTS

RSPs can take the following measures to apply the RBA in the development of remittance products targeting certain groups of customers or business segments to facilitate access to remittance services:

a. Defining certain products, e.g., certain savings accounts, insurance products, mobile wallets, etc., with limited functionality as low risk and marketing them to vulnerable groups such as forcibly displaced people, women and low-income earners.

b. Tailoring specific remittance services with SDD for vulnerable groups such as migrants, including forcibly displaced people, women and low-income earners. This can be done through regulatory approvals.

c. Leveraging on products such as mobile money and digital credit and savings products, which have simplified CDD requirements to provide financial services to marginalized persons such as forcibly displaced people, e.g., for remittances in partnership with donor agencies such as the United Nations High Commissioner for Refugees (UNHCR), and the World Food Programme.

[23] Also see KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries.pdf.

In this regard, mobile money has become an important enabler of financial inclusion in sub-Saharan Africa — especially for women —as a driver of account ownership and usage through mobile payments, savings, and borrowing. It should be fully developed to reach all population segments.

Country Examples of Risk-based KYC for Migrants[24]

1. Pakistan - Most of the population have basic identification (without a photo) held on a centralized ID registration database under the National Registration Authority (NADRA). This includes migrants.

2. Uganda and Kenya - Migrants are required to register and attain a 'refugee ID', which is different from the national ID.

3. Jordan - Refugees are provided with an identification card which has a unique ID. The card is used, together with biometrics (including iris scanning), as a primary key for mobile financial services and SIM card allocation.

4. Tanzania - Identification of refugees is carried out through a letter from the camp director, and a letter from UNHCR. The National Identification Authority also intends to introduce biometrics.

5. Malawi –National Registration Bureau (NRB) announced plans to register and issue ID cards to refugees and asylum-seekers in Malawi.

6. Afghanistan – Refugees can open bank accounts using at least one document, including their driving license, UN migration card, card by international migration organization, card provided by WFP, or card provided by the Ministry of Migration and Returnees. No inward and outward remittance transactions are permitted and monthly turnover on the account should not exceed $100.

ENHANCED DUE DILIGENCE UNDER RISK-BASED APPROACH

1. According to the FATF guidance, RSPs should perform enhanced due diligence (EDD) for higher-risk customers, business relationships or transactions and continuously monitor all high-risk clients.

2. RSPs should identify individual high-risk categories and apply specific and appropriate mitigation measures. Higher-risk scenarios include PEPs, correspondent banking relationships, and cross-border transactions between known terrorism hot spots.

3. While applying the proportionality principle, care should be taken to ensure that the CDD procedures established to comply with CDD requirements are not too demanding for customers wishing to use the services of the RSP.

[24] Also see KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries.pdf.

4. Depending on the circumstances, EDD may take the shape of escalating levels (tiers) of CDD, with higher levels needing the most strict CDD standards, such as escalation of approvals for relationship establishment and increased degrees of relationship evaluation. The intensity and extensiveness of risk management functions should be proportionate to the nature, scale and complexity of the RSP's activities and ML/TF risk profile.

OTHER MEASURES UNDER THE RISK-BASED APPROACH

Other measures that RSPs can take to implement the risk-based approach include the following:

1. Working with regulators to foster innovation by building regulatory sandboxes to test specific new methods of identifying and validating customers and monitoring customer interactions and transactions.

2. Leveraging partnerships with mobile money and other digital financial service providers to foster mobile money and other digital remittance channels with low transaction limits to enhance financial inclusion.

3. Supporting responsible innovation that identifies and addresses associated ML/TF and fraud, security, data, and consumer risks.

4. Collaborating with regulators to assist RSPs with capacity building to foster a better understanding of tiered CDD and risk mitigation to provide services to underserved segments where only simplified customer identity paperwork is available.

CONCLUSION

Remittance services are among the most important channels for driving financial inclusion. They should be fully developed to provide financial access to previously unbanked population segments such as migrants and other vulnerable groups.

However, Remittance services are potentially at risk of being misused for money laundering and financing terrorism activities. RSPs are required to have robust AML/CFT programmes to facilitate compliance with their AML/CFT obligations. However, it is recognized that applying an overly cautious approach to AML/CFT safeguards can have the unintended consequence of excluding legitimate businesses and consumers from the financial system, thereby compelling them to use services not subject to regulatory supervision.

RSPs should, therefore, ensure that they implement AML compliance programmes, which comply with FATF recommendations and applicable AML/CFT legislation while adopting risk-based approach measures outlined in this guidance and in the FATF Guidance Notes and relevant national regulations to support financial inclusion through the use of remittance channels by underserved segments of the population.

KEY REFERENCES

1. Financial Action Task Force Recommendations (updated March 2022) FATF recommendations.

2. FATF Guidance on AML and CFT measures and financial inclusion with a supplement on customer due diligence (fatf-gafi.org) 2017 FATF Guidance on AML/CFT measures and financial inclusion

3. FATF Guidance for a Risk-Based Approach for Money or Value Transfer Services (2016). RBA-moneyvalue-transfer-services.pdf

4. FATF High-Level Principles and Procedures on the Risk-Based Approach (2007). FATF High-Level Principles and Procedures on the Risk-Based Approach.pdf.

5. FATF Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services (2013) FATF RBA-NPPS-2013.html.

6. FATF Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers (2021) FATF Guidance – RBA - Virtual Assets and VASPS.

7. Proportional risk-based AML/CFT regimes for mobile money: A framework for assessing risk factors and mitigation measures, GSMA (2015) Proportional-risk-based-AMLCFT-regimes-for-mobilemoney 2015.

APPENDIX A: SAMPLE RISK RATING MATRIX AND RISK ASSESSMENT TEMPLATE

RISK RANKING (IMPACT AND LIKELIHOOD)

ML/TF risks are recognised and classified as high/medium/low based on the risk's severity, likelihood, and impact using the criteria established to assess the risk to customers and products. The impact assessment below is a guide based on existing measures such as regulatory reforms and political goodwill.

- Low: The risk is insignificant and can be managed with routine procedures.
- Medium: The risk is significant but manageable with additional controls or mitigations.
- High: The risk is severe and requires immediate attention and action.

Sample Risk Rating Matrix

Risk Factor	Indicators	Impact	Likelihood[25]	Ranking/ Comments[26]
Geographic or country risk	• Porous borders • Internal political instability • External political instability • Widespread corruption in the public sector • Lack of political goodwill • Prevalence of financial crime • Thriving black/unregulated market for smuggled goods through porous borders • High poverty levels	H		
Financial services or product risk	• Product risks - speed, anonymity and simplified CDD requirements	M		
Financial exclusion/customer risk	• Informal cash-based/grey economy • Inadequate identity registration and CDD processes for forcibly displaced and undocumented persons	MH		
Institutional and third-party risk	• RSPs doing business with non-compliant entities/third parties	L		
Compliance risk	• Low compliance levels, i.e., non-compliant reporting institutions with inadequate AML compliance programmes	MH		

[25] Likelihood depends on the identified risk factors in each country.

[26] Ranking should be based on existing mitigatory measures in place to reduce the risk.

Risk Factor	Indicators	Impact	Likelihood[25]	Ranking/ Comments[26]
System delivery and channel risks	• Mobile money, Internet payments, and other digital financial services facilitate anonymous transactions which are difficult to track	MH		
Regulatory and Legal Risk	• Regulatory gaps - no implementing regulations for the Money Laundering and Prevention of Terrorism Financing Act, regulatory capacity challenges, inadequate supervisory resources, e.g., monitoring informal cash transactions and non-compliant institutions	M		

Sample Risk Assessment Template

RISK	AREAS AFFECTED	SEVERITY	LIKELIHOOD	RISK IMPACT	EXISTING MITIGATORY MEASURES	RECOMMENDED ACTION(S)

Note: The recommended actions should address gaps noted in the existing measures

APPENDIX B: CASE STUDY

ABC Money Transfer

ABC Money Transfer is a medium-sized non-bank RSP operating in Country X. It is registered as a corporate entity under the Companies Act and is licensed to provide money transfer services by an authority recently set up to oversee the activities of money transfer businesses in Country X.

ABC's customers are primarily locals who send and receive remittances. However, it also serves migrants who receive remittances from their relatives in the diaspora for maintenance and support or cash aid from donor organizations such as the UNHCR and the World Food Programme. Some of these migrants are also involved in small-scale cash-based businesses and send money to relatives in their countries of origin. The migrants are mainly from neighbouring countries Y and Z, experiencing political conflict for several years. ABC has various partnerships with banks and mobile money providers regulated by the Central Bank for the use of their platforms.

Country X has a relatively stable government with a largely cash-based informal economy. However, corruption is rampant, and legislative reform is very slow. There is also a thriving black market for goods and foreign currencies coming into the country through porous borders facilitated by poor immigration controls at the borders. Country X has high poverty levels among local and migrant populations, and financial crimes are prevalent.

Country X has AML/CFT legislation in place, and licensed RSPs, including money transfer businesses, must report suspicious activity to comply with the AML Act. However, there are no specific AML/CFT regulations for RSPs.

The AML/CFT law does not provide for a risk-based approach to CDD measures for migrants. However, Country X legislation concerning forcibly displaced people recognizes migrants and provides for identity refugee cards to be issued to migrants, as well as temporary residency status permits.
Most migrants lack bank accounts because they lack the CDD documentation banks require. However, a number of them have mobile money wallets.

ABC has an AML Compliance Officer but does not have an automated transaction monitoring and sanction screening system and has not carried out an AML/CFT risk assessment.
ABC wishes to expand its products and services offered to migrants and to carry out a risk assessment to develop a KYC policy document for migrants.

How would ABC assess the ML/TF risks using the sample risk matrix below?

ABC Money Transfer: Sample Risk Rating Matrix

Risk Factor	Indicators	Impact	Likelihood	Comments
Geographic or country risk	• Porous borders • Internal Political Instability • External political instability • Rampant corruption in the public sector • Lack of political good • Prevalence of financial crime. • Thriving Black/unregulated market for smuggled goods through porous borders • High Poverty levels	H	M	The country has porous borders, an informal cash economy and a thriving black market. There are also gaps in the law
Financial services or product risk	• Product risks - speed, anonymity and simplified CDD requirements	M	M	Whereas there are no SDD provisions for migrants, ABC has an AML compliance programme and deals with regulated third-party partners. Its transactional volumes are also moderate
Financial exclusion/customer risk	• Informal cash-based/grey economy • Inadequate identity registration and CDD processes for refugees and undocumented persons	MH	MH	While ABC has an AML compliance programme, it may experience challenges in vetting its customers and establishing the source of funds
Institutional and third-party risk	• RSPs doing business with non-compliant entities/third parties	MH	ML	ABC deals with third-party partners regulated by the central bank
Compliance risk	• Low compliance levels - non-compliant reporting institutions with inadequate AML compliance programmes	MH	M	ABC has an AML Compliance programme; however, needs to put in place additional controls

Risk Factor	Indicators	Impact	Likelihood	Comments
System, Delivery and Channel Risks	• Mobile money, Internet payments, and other digital financial services facilitate anonymous transactions which are difficult to track	MH	M	ABC offers its services through regulated third-party partners regulated by the central bank
Regulatory and Legal Risk	• Regulatory gaps - no implementing regulations for the Money Laundering and Prevention of Terrorism Financing Act regulatory capacity challenges, inadequate supervisory resources, e.g., monitoring informal cash transactions and non-compliant institutions	M	M	There is an AML Act, and while there are no regulations for RSPs, the requirements under the Refugee Act can be leveraged to provide services to migrants

H- High, M – Medium, L – Low, MH – Medium to High, ML – Medium to Low

Note: The recommended actions should address gaps noted in the existing measures

ABOUT UNCDF

UNCDF mobilizes and catalyzes an increase in capital flows for SDG impactful investments to Member States, especially Least Developed Countries, contributing to sustainable economic growth and equitable prosperity.

In partnership with UN entities and development partners, UNCDF delivers scalable, blended finance solutions to drive systemic change, pave the way for commercial finance, and contribute to the SDGs. We support market development by enabling entities to access finance in high-risk environments by deploying financial instruments, mechanisms and advisory.

For more information, please contact:
Albert Mkenda
albert.mkenda@uncdf.org

Follow @UNCDF