Risks facing remittance service providers

A risk management framework for policymakers and regulators

© 2025, United Nations Capital Development Fund (UNCDF) All rights reserved worldwide

The views expressed in this publication are those of the author(s) and do not necessarily represent the views of UNCDF, the United Nations or any of its affiliated organizations or its Member States.

All queries on rights and licences, including subsidiary rights, should be addressed to:

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, and their wider communities in least developed countries, the UNCDF Migration and Remittances 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 risks facing remittance flows. This appreciation is not their endorsement of this paper and is extended to a number of 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 the financial and remittance industries, research participants, regulatory and policymaking leaders, and many other individual or organizational stakeholders.

The drafting of this risk management framework was led by Albert Mkenda, remittance policy specialist, with invaluable inputs and support from Amani Itatiro, Doreen Ahimbisibwe, Mercy W Buku, Uloma Ogba. 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. Eliamringi Mandari and Amil Aneja 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 Migration and Remittances programme has been made possible by generous funding support from the Swiss Agency for Development and Cooperation (SDC) and from the Swedish International Development Cooperation Agency (Sida). 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.

CONTENTS

ACRONYMS AND ABBREVIATIONS

AML	anti-money laundering
AML/CFT	anti-money laundering/countering financing of terrorism
BoP	balance of payment
CDD	customer due diligence
ECCAS	Economic Community of Central African States
e-KYC	electronic know your customer
FATF	Financial Action Task Force
GP	General Principles for International Remittances Services
ID	identification
IGAD	Intergovernmental Authority on Development
ISO	International Organization for Standardization
KYC	know your customer
ML/FT	money laundering/ financing of terrorism
RBA	risk-based approach
RSP	remittance service provider
UNCDF	United Nations Capital Development Fund

1.0 | INTRODUCTION

Due to the constantly changing business environment, the need for an effective risk management framework for remittance service providers (RSPs)1 cannot be over-emphasized. Through effective risk management, RSPs must be able to mitigate risks and optimize their risk-return trade-off for the safety and soundness of the remittance sub-sector within the broader financial market. In response to the ever-changing business environment, a more risk-based approach (RBA) to remittance services must be adopted, one that focuses on identifying risks and assessing the management of the risks. To enable this, regulators must put forward a guide to provide a framework to all RSPs on the minimum requirements for risk management practices. Moreover, regulators must be able to come up with an appropriate risk assessment methodology that can be used for supervision of the RSPs.

2.0 | OBJECTIVE OF THE FRAMEWORK

The main objective of this framework is to assist policymakers in policy formulation and regulators in issuing guidelines to market players in the remittance space for identifying, evaluating, monitoring, and controlling key risks facing the RSPs. This framework can also be used as a supervisory tool for regulators and help to strengthen the policymakers' capacity to develop gender-responsive and risk-based remittance policies that enhance market competition and innovation while safeguarding against risks to financial stability. In this regard, it makes it easier for policymakers and supervisors to strike a balance among the policy objectives of financial inclusion, stability, integrity, competition, and consumer protection. Effective risk management for the remittance market is in line with encouraging key players to address the frictions that cause the remittance challenges of high cost, limited speed, transparency, and access. A risk-based approach in conducting supervisory activities on remittance market can optimize resources and improve risk management practices, leading to reduced compliance cost and improved usage and access to remittance services. This is because it enables the regulator to tailor the type, scope, and depth of their supervisory activities focusing resources on the most significant risks. Moreover, this framework can be used by Member States of regional economic communities as a tool for harmonizing policies and regulatory frameworks relating to remittance markets' risk management.

Actions of policymakers and regulators can affect the RSPs' risks management practices, either positively or negatively, particularly when formulating policies, supervisory frameworks, and tools relating to the following:

i. Licensing, supervision, and supervision of RSPs and payment systems providers
ii. Maintaining financial integrity and risk management
iii. Ensuring consumer protection and complaints resolution mechanisms

[1] In this framework, RSPs include banks and non-bank money transfer operators (MTOs). Non-bank MTOs include larger international firms that offer a global remittance service through a network of agents, ATMs, mobile money operators, and electronic channels worldwide, as well as a wide range of smaller organizations that concentrate on sending money across specific migration corridors or through digital channels.

iv. Monitoring foreign exchange operations
v. Overseeing the operation of payment systems
vi. Improving the payment ecosystem, etc.

With new technologies and business models, the risk profiles of RSPs may vary and constantly change depending on the focus. Areas of focus that may shape risks in remittance services include operational resilience, governance, liquidity management considerations, investor and consumer protection, broader monetary and financial stability considerations, banking regulations, AML/CFT compliance, data security, privacy, and confidentiality considerations. Policymakers and regulators could consider contributing to the stability of the RSPs' operating environment and effective risk management practices through their actions in these areas, given their ability to create desired changes or bring unexpected uncertainties and risk exposures. Policymakers and regulators could ease the management of cross-border risks and uncertainties via the following means:

a. Facilitate cross-border engagements and cooperation. These are necessary to address potential exposures and policy issues relating to cross-border payments in supporting the safety and efficiency of remittance services. Cooperation and coordination are, in addition, essential for the interoperability of the payment infrastructures and thus improve the abilities of infrastructures to offer a reliable unit of account, payment finality, and adequate liquidity for settlement regarding cross-border payments.

b. Facilitate access to and sharing of cross-border information. Legal risks increase when there is inadequate cross-border access to information for regulatory and supervisory purposes. Cross-border access to information is essential to successfully and efficiently regulating and supervising cross-border payments. Due to the nature of remittance services, effective risk management necessitates sharing information that may span numerous jurisdictions and with regulatory authorities in other countries for cross-border supervision and supervision. To manage ML/FT risks, for instance, the AML/CFT regulations mandate cross-border information sharing within financial groups. Policies restricting cross-border data flows may make monitoring and supervision more challenging and thus increase risks for RSPs and payment systems.

c. Commit to uniform or similar or regional and international regulatory and supervision systems. Operational risk increases when different regulatory and supervision systems govern cross-border payments. Regulatory and licensing requirements may vary depending on the jurisdiction. The effectiveness and efficiency of supervision over cross-border payments may be exposed to variations in domestic regulation and supervision across jurisdictions, particularly if they fall short of international standards. This raises the possibility of regulatory gaps in the supervision of cross-border arrangements. Policymakers and regulators should strive to apply international norms uniformly at the domestic level to effectively achieve coordinated risk management practices. The risks mentioned in this framework, i.e., technological, compliance, reputation, foreign exchange, interest rate, credit risk, and liquidity risk, may all be made worse by an uneven implementation of international standards.

d. Pioneer interoperability. Technological risks may be increased by the lack of interoperability across jurisdictions. As a result, RSPs must incur high costs on technology and operational procedures for each market or currency zone they serve. The public authorities' involvement in these aspects can entail encouraging the application of globally accepted technological standards and increased interface standardization.

e. Mandate coordination among market players. Coordination among players on innovations can reduce the payments market's fragmentation and hence reduce technological risks. Individual RSPs may innovate, but more coordinated innovation may occur through multilateral payment systems. Innovations by the private sector in cross-border payments can be more effective if public agencies act as catalysts and facilitators. Coordination also improves uniform reporting on incidents and risks facing the market players.

f. Develop policies to increase currency convertibility. When payments are transferred across borders from a sender in one currency to a recipient in another, risks involving foreign exchange, liquidity, and legal duties arise. When dealing with RSP risks, the point of forex conversion, the forex conversion rate, and the requirement to maintain compliance with currency regulations and capital account controls are all critical considerations. In addition, cross-border payment flows between countries may not be equal in total value, incurring balance of payment (BoP) issues.

The policymakers and regulators must ensure the right policies, legal and regulatory frameworks. Risk exposures or triggers can be addressed with appropriate policies, legal and regulatory frameworks.

3.0 | REMITTANCE SERVICES CONTEXT

Migrant remittances are cross-border retail payments[2] that migrant workers send to their country of origin to support their families and pay for healthcare, education, etc. In this regard, remittances are important sources of financing and play an important role in economic growth. Over the years, the remittance business has experienced enormous expansion. Remittance service providers include banks, money transfer companies, mobile money companies, and other fintech firms. In most cases, the remittance business is regulated by laws and rules intended to protect customers, guarantee the security of transactions, and fight against money laundering and terrorist financing.

Remittances are typically between individuals, i.e., person-to-person (P2P). In some cases, migrants can transfer funds to purchase services, goods, or utility services for their beneficiaries directly. These are payments to businesses and government agencies, i.e., person-to-business (P2B). Remittances can also be business-to-person (B2P), such as insurance and pension payments to migrants who have relocated. However, in volume and value terms, the most frequent types of remittance payments are person-to-person (P2P) and person-to-business (P2B).[3]

[2] Throughout this report, the focus is on remittances as retail cross-border payments.

[3] Financial Stability Board (2020), Enhancing Cross-border Payments - Stage 1 report to the G20. Financial Stability Board (fsb.org), (accessed on 1 March 2023).

Challenges associated with sending remittances vary widely across country corridors,[4] types of RSPs, and gender of the customers, partly due to the different risk landscapes and types. For instance, most international RSPs avoid remittance business in corridors with high money laundering risks. This has the effect of reducing competition and perpetrating unregulated channels that also come with high costs. Moreover, customers avoid using RSPs which they perceive as having higher chances of loss of money, exploitation and abuse, or cultural and social barriers.

3.1 REMITTANCE SERVICE BUSINESS PROCESSES

Remittance business processes can be a source of risks. To better identify the risks facing remittance services, RSPs can be required to map out all the business processes. All risks facing an RSP are inherent to or originate from the remittance business processes. The formal channels involve distinct processes, including application, application processing, settlement, and payment. Different RSPs have different instructions but generally follow the same process. A study of the business processes is a starting point for identifying and mapping out all the risks pertaining to the RSP.

3.2 PAYMENT METHODS AND CHANNELS

Policymakers and regulators must be mindful that remittance service processes and the associated risks are further influenced by the channels in use and the mode of payment. Remittances can occur through decentralized arrangements, correspondent banking, centralized platforms, or interconnected platforms of RSPs in different countries. The channels may sometimes be combined. For instance, RSPs participating in a correspondent banking arrangement may employ interconnected platforms across national payment infrastructures, where possible, to increase efficiency and cut costs. The availability of multilateral cross-border payment systems and other circumstances, such as a monetary union, may substantially impact the channels used in different countries. Knowledge of the mode of payment is critical for effective risk management.

These modes of payment and channels involve payment systems, compliance with legal and regulatory frameworks, and payment instruments, all of which can lead to risk exposures.

3.2.1 Payment Systems

In some of these modes of payment, payment systems are used to conduct transactions. Moreover, multicurrency settlement systems offer centralized infrastructures that RSPs can use to settle foreign exchange transactions. These systems typically work on a payment versus payment (PvP) basis,[5] although bilateral settlement agreements are also available. Typically, these systems employ various messaging protocols and formats, which has been one of the sources of operational risks.

[4] The "country corridor" in this framework means money flows between two countries or regions.

[5] A settlement procedure that ensures that the final transfer of a payment in one currency occurs only after the final transfer of a payment in another currency or currencies.

3.2.2 Legal Frameworks

Certain legal and regulatory frameworks are important because they govern the payment agreements or schemes entered into among RSPs to enable processing, clearing, and settling cross-border payments. Typically, RSPs may enter into bilateral or multilateral agreements, including operational and commercial rules and agreed-upon technical standards that participating RSPs agree to abide by. Moreover, several countries' legal and regulatory frameworks, including those pertaining to consumer protection, cyber-security, licensing and authorization requirements, prudential supervision (including risk management), and AML/CFT frameworks, come into play. Most often, regulatory frameworks may differ on transaction thresholds, the categories of entities permitted to conduct cross-border payments and the conditions for obtaining a license, submission of returns and reports to the regulators, BoP calculations, and sanctions laws. RSPs may therefore encounter challenges in locating comprehensive information on the nature of compliance requirements and become vulnerable to the interpretation and application of those regulations.

3.2.3 Payment Instruments

Payment instruments used during the remittance processes can also influence the risk profile of an RSP. Senders and recipients of remittances can use various payment methods, including cash, credit and debit cards, electronic fund transfers, and e-money, such as mobile money. The instrument used depends on the RSP, the jurisdictions or regions involved in the transaction, and the type of end-users in question. Physical cash can, for example, cause insecurity and increase money laundering risks. Technological risks increase with electronic fund transfers, e-money, etc.

RSPs must be required to methodically categorize and define all possible risks that manifest in the RSPs' business processes and payment channels to ease risk assessment, mitigation, monitoring and control, and communication.

4.0 | KEY RISK CATEGORIES FACING REMITTANCE SERVICE PROVIDERS

The relatively small values involved in remittance transfers mean that it is unlikely for RSPs to pose systemic risks. However, at an individual level, RSPs face liquidity, forex exchange, interest rate, and reputational risks.[6] RSPs could face risk factors from human actions, technological deficiencies, and market operations with inadequate transparency and weak legal and regulatory frameworks. A comprehensive definition and scope of key risk categories RSPs may face is key but should be proportional to the RSP's business size.

4.1 LIQUIDITY RISK

This is exposure to RSPs arising from their inability to meet their obligations as they fall due or failure to fund asset growth without incurring unacceptable expenses or losses. Liquidity risk includes the exposures from the inability to manage unplanned decreases or changes in funding sources. In the situation of

[6] Bank for International Settlements & The World Bank, (2007). General principles for international remittance services. Available on the websites of the BIS (www.bis.org) and the World Bank (www.worldbank.org).

failure to meet such obligations, an RSP often depends on the market for liquidity requirements. However, market funding conditions depend on the market's general liquidity and the RSP's creditworthiness. In this regard, RSPs may not receive payment on time and must borrow or liquidate some of their assets to complete other payments. The failure or inability of settlement banks, nostro agents,[7] custodian banks, liquidity providers, and associated payment infrastructures to perform as planned can also be other sources of liquidity risk.

Borrowing funds to provide liquidity is costly. These cost elements can lead to high barriers to entry and an unwillingness to do business with less profitable customers, such as low-income migrants, limiting their access to remittance services. RSPs must ensure they have enough liquid assets to meet their consumer's eligible demands and complete transactions with their correspondents. Transactions that are delayed or cancelled due to a lack of liquidity may harm an RSP's reputation and its customers' trust.

In principle, liquidity risk should not be seen in isolation because financial risks are not mutually exclusive. The consequences of other financial risks, such as credit, interest rates, and foreign exchange, may often trigger liquidity risk.

4.2 FOREIGN EXCHANGE RISK

Remittance transfers frequently involve foreign exchange transactions. Usually, the exchange rates fluctuate from time to time due to various factors in the financial markets. RSPs can be in a situation where the exchange rates may have unfavourably changed when converting funds from the sending country's currency to the receiving country's currency. Exchange rates may also change with time from when a customer applies for a transfer to the payment and settlement date. The uncertainty an RSP experiences from the exchange rate changes makes the amount due by the RSP on the payment date different from the amount due on the settlement date.

Another foreign exchange risk arises when an RSP has a foreign subsidiary or agent whose reporting currency differs from the parent RSP's reporting currency. In this regard, the subsidiary RSP or agent balance sheet items are converted for consolidation purposes into the parent RSP's reporting currency, which can result in changes in the consolidated financial position and earnings.

Changes in exchange rates can affect the profitability of transactions and cost to the final consumers. An RSP must be required to manage these risk factors through hedging strategies and deploying proper risk management guidelines.

4.3 INTEREST RATE RISK

Interest rate risk is the potential for losses in on- and off-balance sheet positions because of adverse changes in market rates and fees. Changes in interest rates can also affect the profitability of transactions and costs chargeable to the final consumer. RSPs must manage these risk factors by deploying proper risk management guidelines.

[7] A nostro account refers to an account that a bank holds in a foreign currency in another bank.

4.4 CREDIT RISK

Credit risk arises from exposures from a counterparty unwilling to perform an obligation or its ability to perform such obligation is impaired, which may result in economic loss to an RSP. Since the chain transactions do not occur in a sequence, the receiving agent may disburse funds to the final beneficiary customer before the sending RSP initiates the settlement process.

The "paying before being paid" situation, in which most RSPs risk losing money, is a major source of credit risk. A transferring RSP might agree with the disbursing agent that liquidity will be available for the agent to pay the recipient as soon as the message is received or at a specific time. The disbursing RSP takes on credit risk in this case. Particularly for franchised RSPs,[8] the recipient occasionally has a choice regarding where to pick up the money. In this case, the RSP might not know which disbursing agent to pay until the money has been collected unless there is a strong management information system. If there is no liquidity agreement between them, the disbursing agency may be exposed to credit risk. Another type of credit risk exposure is the likelihood that an RSP, like a bank, provides services in addition to remittances. In the normal course of business, they may accept payments and extend credit. Credit risk may result in liquidity risk.

4.5 OPERATIONAL RISK

Operational risk is exposure from inadequate or failed RSPs' internal processes, people, systems, or external events that may lead to limited, deteriorated or breakdown of services causing losses or decline of earnings and capital. Internal and external factors can contribute to operational risks. Processing mistakes or delays, lack of proper documentation, poor management, lack of or inadequate contingent plans, lack of or inadequate policies, procedures, and controls, inefficiencies in information systems or internal processes, system breakdowns, insufficient capacity, fraud, data loss and data leakage are a few examples of potential internal operational failures. An example of external factors is when participants of a payment system, for instance, create operational risk for other participants, which may cause issues with liquidity or other operational problems to them.

Internal and external exposures may cause technology breakdown, cyber-crimes, poor contracting, poor contract enforcement, disproportionate and discriminatory licensing procedures, disproportionate prudential supervision, poor financial integrity, ineffective risk management practices, inadequate consumer protection, and disproportionate forex regimes. In addition, operational risks such as money laundering/financing of terrorism (ML/FT) may be inherently higher because remittance services involve non-face-to-face business relationships or transactions.

All these risk factors can, in turn, result in substantial financial losses to the RSP and disruptions to other RSPs in the same payment system, leading to undermined public confidence in the safety, soundness, and reliability of the remittance services. This can lead to informal channels of sending remittances.

[8] A franchised service is one in which a central provider builds infrastructure to support the remittance service but acquires the required access points by inviting institutions in both sending and receiving countries to offer the service or operate as franchisees on standardized terms.

The RSPs must properly categorize operational risk for ease of management. Four sub-categories include compliance (legal), country (political), technological, and strategic risks.

4.5.1 Compliance Risk

The possibility that legal action will be taken against an RSP because of the RSP's actions, inactions, products, services, or other events brings in the possibility of potential non-compliance with legal and regulatory frameworks. Disjointed regulatory regimes, including AML/CFT, sanctions screening and combatting financial crime, may increase the exposure to this risk. Actions or inactions leading to omission may result in regulatory penalties and sanctions. Compliance risks impact the earnings, capital, and reputation of an RSP.

This risk category includes legal risks, i.e., misinterpretation of policies, laws and regulations, and unexpected or uncertain application of a law or regulation that may result in a loss to the RSP. In extreme circumstances, legal risk may render contracts unenforceable, resulting in a loss from a delay in the recovery of financial assets or a freezing of positions because of a legal procedure.

An RSP is usually subject to various compliance requirements from the regulations on licensing, foreign exchange management, consumer protection, anti-money laundering and counter-terrorism financing, privacy and data protection, electronic money, submission of returns to the regulator, and many others. Failure to comply with these regulations can result in penalties, reputational damage, and even cessation or closure of business.

Compliance risk can result in license revocation, financial penalties, the payment of damages, a decline in market share, and a restricted capacity for expansion. Compliance risk can also result in reputational risk. This could hinder an RSP's capacity to develop new connections, offer new services or goods, or maintain existing connections. Moreover, RSPs may be subject to administrative, civil, and criminal liability leading to financial loss or a decrease in customer base.

4.5.2 Country Risk

The exposures RSPs may face when doing business in a foreign jurisdiction are called "country risks." Such risks can also arise from conducting business or lending or borrowing money internationally. Political, legal, and regulatory aspects that vary between monetary unions or countries may also pose country risks.

4.5.3 Technological Risk

Technological risks include technology-related failures or occurrences that could harm people, other RSPs, society, or even the RSP itself. Factors that could expose an RSP to technological concerns include system breakdowns and errors due to deploying complex IT systems that enable transactions. Others include the use of unproven or unreliable hardware, software, or infrastructure, improper maintenance, human mistakes, misbehaviour, cyber-attacks, cybersecurity breaches, system failures, technological catastrophes, improper IT projects management, failure of critical systems, such as power grids or transportation networks, due to technical malfunctions or cyber-attacks, and hacking. These accidents may lead to data loss, equipment damage, and disruption of essential systems and services. Any of these

incidents may affect the reliability and speed of remittance transactions. Technological risks can have substantial financial and reputational implications for an RSP, including the loss of revenue, regulatory fines, and damage to brand reputation.

4.5.4 Strategic Risk

Strategic risk is the possibility that an RSP would experience losses or other consequences for failing to achieve its strategic aims and objectives. This may result from several internal or external factors that hinder an RSP's ability to achieve its goals. This risk is a function of the compatibility of an RSP's strategic goals, the business strategies developed, resources employed to achieve strategic goals, and the quality of implementation of those goals. External elements are the ones that can have an impact on or prevent the achievement of the goals outlined in the strategic plan and are either difficult for the RSP to control or that the RSP has no control over, such as competition, shifting consumer markets, and global or regional or national economic conditions. All these occurrences may result in market share and/or monetary losses.

4.6 REPUTATION RISK

The reputation risk is any potential for damage to an RSP's brand and image by negative events that could result in, among others, a loss of customers and income. Reputation risk factors include an RSP's failure to have sufficient plans to guarantee that recipients receive their monies on time, even if there has been a loss in transit. Also, using the service illegally, for instance, for drug trafficking, human trafficking, or money laundering, may result in reputational risk.

5.0 | RISK MANAGEMENT GUIDELINES

Despite the consequences of these risks to an RSP, their effects can also extend to the RSP's customers if not properly managed. Major consequences to customers of remittance services include the following:

i. Loss of money in transit
ii. Fraud or scams such as phishing or identity theft
iii. Unfavourable exchange rates since the value of the transmitted currency may vary
iv. Higher service charges, i.e., remittance service providers, may bill customers for their services with exorbitant fees and commissions
v. Delays or other delivery issues

In this regard, customers exercise due diligence when selecting an RSP and consider aspects such as speed, outreach, security measures in place, reputation, adequate disclosure of all costs, exchange rates and fees, license status, regulatory compliance, information about customers' rights and obligations when utilizing remittance services, and available precautions to safeguard customers' financial and personal data. Therefore, Risk management practices are paramount for an RSP's sustainability and profitable operations. Ultimately, risk management reduces the cost of remittances, increases efficiency, and improves access to remittance services. It is a supervisory objective to mandate RSPs to have good risk management guidelines for the safety and soundness of the remittance sub-sector.

When developing risk management guidelines, it is important to note that the formality and sophistication of risk management frameworks should be commensurate with an RSP's size and risk profile.

Apart from the UNCDF diagnostic reports,[9] RSP guidelines for risk management can be informed by a review of several global standards and principles, some of which include the following:

i. General Principles for International Remittances: The General Principles for International Remittances Services (GPs), among others, recommend adequate governance and risk management practices critical to the RSPs.[10] The GPs urge a thorough examination and study of the major frictions that lead to the remittance challenges of high cost, slow speed, limited access, and transparency. Furthermore, GPs pinpoint potential sources of legal, operational, fraud, and reputational risks and how to address them. The GPs urge adequate governance and risk management practices to ensure less friction in the remittance channels. A solid, predictable, non-discriminatory, and appropriate legal and regulatory framework in the applicable jurisdictions must back remittance services.

ii. Financial Action Task Force (FATF): The Financial Action Task Force (FATF)[11] leads global action to tackle money laundering, terrorist and proliferation financing and supports global standards to mitigate risks from illicit funds linked to drugs trafficking, illicit arms trade, cyber-fraud, and other serious crimes. Furthermore, FATF publishes reports that raise awareness about the latest money laundering, terrorist financing and proliferation financing techniques so that countries and the private sector can take the necessary steps to mitigate these risks. FATF recommendations[12] support implementing legal, regulatory, and operational measures for combating money laundering, terrorist financing, and other related threats to the integrity of the international financial system. Guidelines for addressing technological remittance risks include ML/FT risk reduction in digital payment ecosystems, data enhancement, and AML/CFT reporting.

iii. Principles for Financial Market Infrastructures: Payment infrastructures are critical for remittances. However, they may be a major source of operational risks that RSPs may face. The Principles for Financial Market Infrastructures discuss the systemic risk and other key risks facing Financial Market Infrastructures, i.e., legal, credit, liquidity, general business, custody, investment, and operational risks. These principles advocate for identifying plausible sources of operational risk, both internal and external, and mitigating their impact using appropriate systems, policies, procedures, and controls. Payment systems should provide comprehensive and appropriately detailed disclosures to improve the risk management framework. The main focus should be on efficiency and effectiveness, meeting the requirements of their participants and the markets they serve while maintaining appropriate safety and security standards.

---

[9] Research - Migrant Money (uncdf.org)

[10] General Principles for International Remittances Services - Financial Stability Board (fsb.org) (accessed on 17 February 2023)

[11] What we do (fatf-gafi.org) (fatf-gafi.org) (accessed on 17 February 2023)

[12] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html (accessed on 17 February 2023)

iv. International Organization for Standardization: Messaging standards in use may pose operational risks to RSPs. Standardized messaging formats and reference data standards for identifying financial instruments and counterparties in line with ISO standards, especially ISO 20022 on messaging, are preferable. Using internationally accepted standards for message formats and data representation generally improves the quality and efficiency of the clearing and settlement of financial transactions. Lack of straight-through-processing and most reconciliation problems originate from using different incompatible messaging standards.

v. Payment Card Industry Data Security Standards: Data security is an important remittance services component and, if not properly considered, may pose reputational and operational risks to an RSP. These standards focus on increasing controls around cardholder data and reducing credit card fraud risks.

vi. G20 High-Level Principles on Digital Financial Inclusion and Plan to Facilitate Remittance Flows: Digital innovation with the new risks from the rapidly evolving technology must be well balanced. The principles advocate for balancing innovation to achieve digital financial inclusion with identifying, assessing, monitoring, and managing new risks. In 2014, the G20 announced its G20 Plan to Facilitate Remittance Flows.[13] This plan includes an outline for country-led actions to support reducing remittance costs.

5.1 GENERAL RISK MANAGEMENT GUIDELINES

The risks facing RSPs can be substantial and must be carefully managed to ensure its operations' reliability, security, profitability and, ultimately, good remittance services to customers, including women and men migrants and their families. This requires a strong focus on compliance, operational resilience, and proper management of liquidity, credit, interest rate, and foreign exchange operations while protecting the reputations of RSPs.

5.1.1 Environmental Scanning

Risk management guidelines issued by regulators or supervisory authorities must require RSPs to identify external and internal risk concerns when formulating risk management standards.

External Environment

External risk factors must be scanned thoroughly, and respective risk management techniques should be available. The external environmental risk factors include the following:

i. **Competition**: Intense competition, if not carefully managed, can expose an RSP to risks. In this regard, strategic and business plans must align with current and anticipated future competition. Competitive factors must be considered when developing RSPs' risk management guidelines and new products.

13 https://www.gpfi.org/publications/g20-plan-facilitate-remittance-flows

ii. **Change of Target Customers:** Changes in demographics and consumer profiles may affect the customer base, earnings, and capital funding of an RSP. When evaluating the possibility and potential consequences of risks, RSPs should consider how risks may disproportionately impact migrants and gender. For example, if a risk event leads to a disruption in remittance flows, women may be more vulnerable to the economic consequences of this disruption due to their higher reliance on remittances for household expenses.

iii. **Technological Changes:** Due to changing technologies, RSPs may fail to properly position themselves or perform well in the market. At the same time, their competitors could develop more efficient systems or services at lower costs. RSPs should ensure that the level of technology in use is sufficient and up to date with industry standards to provide efficient and effective remittance services and retain its customer base.

iv. **Economic Factors:** Global, regional, or national economic conditions affect the level of profits of an RSP leading to effects on the liquidity, exchange rate, credit, and operational risk profiles. Consequently, continual assessment and monitoring of economic trends and forecasts are critical in developing and maintaining good risk management guidelines.

v. **Policy and Regulations:** Changes in laws and regulations governing the financial sector, tax regime, and other regulatory authorities and agencies may affect the risk profile of an RSP and the implementation of its strategic and business plans. RSPs may require adjustments to the reporting systems and plans to ensure compliance.

Internal Environment

RSPs should also be mandated to scan internal environmental risk factors. These include the following:

i. **Organizational Structure:** An organization's structure is important for implementing strategic and business plans and meeting overall goals most efficiently. A poorly designed structure may pose substantial operational risks. In this regard, an RSP must establish a clear organizational structure. The organizational structure of an RSP should be consistent with its plans and reduce conflicts of interest among its shareholders, board of directors, management personnel,[14] and staff.

ii. **Work Processes and Procedures:** These enable timely and accurate implementation of business plans. If not appropriately handled, they may lead to operational exposure to an RSP. The board of directors should establish responsibilities and clear guidelines, policies, and procedures to prevent work-related deficiencies.

iii. **Information:** Most RSP exposures could be reduced with a swift and timely flow of information. On the other hand, a lack of adequate, relevant, accurate, and timely information exposes RSPs to various

[14] Management personnel means and includes the Chief Operating Officer (COO) or equivalent position and other senior personnel positions designated as management positions by the board from time to time.

risks. A thorough understanding of the market has a favourable impact on creating business strategies and developing risk management guidelines.

iv. **Technology:** Technology systems can potentially be sources of operational risk for RSPs. Technology systems must manage the volume of transactions and all client requests efficiently and effectively to compete and establish new business lines. Technology risk management guidelines are also essential.

v. **Personnel:** The board of directors' knowledge, expertise, and vision, as well as that of management and employees, are critical to achieving strategic and business plans. RSPs should have a knowledgeable board of directors, competent management personnel, and staff with relevant risk management experience. The personnel of RSPs are a source of many risks facing it. RSPs must have risk management guidelines that establish clear lines of authority and responsibility for managing each risk category. A lack of competent and sufficient personnel can increase risk exposures, poor financial results, and reputational harm for the RSP. Personnel should have the necessary knowledge and expertise to perform their duties effectively and efficiently.

It is also critical to ensure diversity, including gender, on boards, personnel, and management so that a broad set of risks that would affect customers can be addressed. The following should be considered:

a. **Board of Directors or its Equivalent:** Understanding the category and degree of each risk an RSP is exposed to ultimately rests on the board of directors. The board should know the RSP's profile and the necessary instruments for managing each risk and must ensure the availability of adequate personnel and infrastructure required to manage the risk in all relevant scenarios. The board should comprise qualified individuals with the necessary qualifications and motivation to perform their duties. Often, non-executive board members must be included, and considerations on gender should be made. The board should have clearly defined roles, responsibilities, and processes for its operations, including identifying, handling, and resolving conflicts of interest. The board should routinely evaluate its overall performance and the performance of each board member.

b. **Management Personnel:** The management personnel of RSPs should demonstrate essential knowledge of each risk and be fully capable of managing it, including adopting the appropriate actions to measure, monitor, and control it. The management personnel must be able to monitor and manage the risks while adhering to the policy approved by the board of directors. The management personnel of an RSP must have the necessary expertise and moral character to carry out their duties concerning risk management and operation and should be responsible for effective internal controls and ethical standards.

c. **Other Staff:** A designated individual or committee inside an RSP with the necessary expertise and an in-depth understanding of the nature, extent, and management of the relevant risk category facing an RSP should oversee that risk category. The staff responsible for each risk category must have the qualifications and expertise to assess and control the relevant exposures facing the RSP. The staff should

be able to generate reports that include both aggregate data and enough supporting information to let management personnel gauge how sensitive the RSP is to changes in market conditions and other substantial variables.

5.1.2 Deployment of Risk Management Tools

RSPs must be required to have key risk management tools. These tools include a strategic plan, a risk management policy, and an operation manual.

Strategic Plan

For day-to-day management, each RSP should have a predetermined strategy for each risk category. The overall approach to the management of each risk category should be outlined in the strategy, along with numerous quantitative and qualitative goals. An RSP's strategy should outline how to safeguard its financial stability and endure adverse market circumstances. The strategy should be formulated after determining the RSP's appetite for each risk category, and the strategy should strike a balance between the corporate objectives and that risk. The RSP should consider the influence of economic conditions while formulating a strategy.

Furthermore, the strategy should help the RSP to determine whether it possesses the knowledge necessary to benefit from a particular situation and the ability to recognize, track, and manage the risk associated with each situation and transaction. Furthermore, the strategy should guide the construction of a portfolio mix to protect the RSP from increased risk. The board of directors should support the strategy for each risk category.

Risk Management Policy

Each RSP should develop a policy to implement the risk management approach for each risk category. The procedures for implementing the policy should be followed at all levels of the RSP and should be communicated in a timely manner. Any breach of the policy provisions must be reported, and appropriate action must be taken. The policy should be consolidated, and certain subsidiaries, agents, affiliates, or units within the RSP should be subject to it if necessary. The policy should explain how each risk category is identified and measured, how the risk appetite for the RSP is determined, how frequently risk limits are reviewed, and how each risk is evaluated. The policy should specify the roles and responsibilities of the board of directors, management personnel, and other individuals in charge of managing each specific risk category and the range of operations the business units that shoulder each risk category are expected to perform. In addition to providing instructions on all of these areas, the policy should clarify the structure of each risk limit, the delegation of approval power for each risk limit and limit excesses, capital requirements, and the investigation and resolution of erroneous or disputed transactions. The policy and processes should be frequently evaluated to make sure they are still acceptable and solid. The policy on each risk category should be reviewed at least once a year, except for unusual situations. Personnel at the RSP must be familiar with the policy and any changes that may be made in response to changing economic conditions and other factors. The policy on each risk category must be distributed throughout the RSP.

Operations Manual

Each RSP should create an operation manual for each risk category to implement the policy. The manual should set up detailed proper protocols, processes, and constraints. The manual must be reviewed and updated regularly to reflect new initiatives and changes to risk management strategies and policies.

5.2 SPECIFIC RISK MANAGEMENT GUIDELINES

Sound governance and risk management practices on the part of an RSP are critical to avoiding or reducing the impacts of the risks. Regulators must require RSPs to have sound risk management guidelines for comprehensively managing all relevant risks they face. Risk management policies, procedures, and systems should assist RSPs in identifying, measuring, mitigating, and monitoring the risks that arise in or are borne by the RSP. Risk management guidelines should be reviewed annually or as and when the need arises.

In the remittance markets, interdependencies exist, and therefore RSPs should go further to examine the substantial risks they face and expose to other entities (such as other RSPs, settlement banks, and liquidity providers) and create the necessary risk management mechanisms to mitigate these risks. The effectiveness of a wide range of recovery or exit options should be evaluated, and each RSP should identify circumstances that could potentially preclude it from being able to perform its essential operations and services as a going concern.

RSPs must formulate specific risk management guidelines for each risk category.

6.0 | RISK-BASED APPROACH FRAMEWORK

Regulators must undertake risk assessment and measurement in the normal course of market supervision. Evaluating the possibility of damage or loss is a key activity following risk assessment and measurement. It entails locating, mapping, evaluating the risks that might have an adverse effect on the RSP, and rating the risk, i.e., figuring out the likelihood and potential impact or consequences of each risk. There are several different risk measurement methods, including quantitative and qualitative approaches. Quantitative methods measure risk using mathematical and statistical models, while qualitative methods rely on expert judgment and subjective assessments. Some typical quantitative risk indicators include the following:

i. Standard deviation, i.e., a measure of return volatility, is frequently used to evaluate the risk of certain assets or portfolios.
ii. Value at Risk (VaR), i.e., a statistical measure that determines, with a certain degree of accuracy, the greatest loss that a portfolio or investment is likely to sustain for a given period.
iii. Expected Shortfall (ES), i.e., to provide a more thorough understanding of the expected loss that exceeds VaR.
iv. Sharpe ratio, i.e., the risk-adjusted performance of various investments, quantifying an investment's excess return relative to the risk-free rate of return.

In this framework, the focus is on the qualitative approach.

6.1 RISK-MAPPING

Risk-mapping is a tool that is used to identify, analyse, and prioritize risks. The primary objectives of risk-mapping include the following:

i. The first objective is to identify all potential risks that could impact RSPs. This involves a systematic review of all areas of the RSP to identify any potential threats, vulnerabilities, or opportunities for improvement.
ii. The second is to assess the potential impact of identified risks on the RSP. This involves evaluating each risk's potential financial, operational, legal, and reputational impacts.
iii. The third is to prioritize risks based on their likelihood and potential impact. This enables the regulator to focus its resources on the most critical risks and prioritize efforts.
iv. The fourth is to advise RSPs to implement risk mitigation strategies to address identified risks. This involves mandating RSPs to develop and implement specific actions and controls to reduce each risk's likelihood and/or impact.
v. The final objective is to monitor and review the effectiveness of risk management strategies and controls. This involves ongoing review and analysis of risk management processes and regular evaluation of the effectiveness of existing controls.

Risks are inherent in RSP activities. Among the most frequent activities carried out by RSPs are liquidity management, foreign exchange management, credit administration, IT management, and ensuring all sorts of compliance. Each activity's type and degree of inherent risks depend on its nature and scope. Risks may also cross over into different functional divisions, and activity may contain several inherent risks on the other hand. Moreover, one risk may trigger another. Therefore, a functional risk matrix must be created to capture and assess all pertinent risks associated with their activities. An example of a functional risk matrix is provided below (**Table 1**).

Table 1: Sample Functional Risk Matrix

		Inherent Risks								External Risks
S/N	Area/Activity	Liquidity	Foreign Exchange	Interest rate	Credit	AML/CFT	Technology	Legal	Strategic	
1.	Liquidity management	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
2.	Cash management	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
3.	Investment in debt securities	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
4.	Placements in other RSPs	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
5.	Borrowing	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
6.	Equity Investments	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
7.	Foreign exchange trading	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
8.	Management information system	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
9.	Cash in bank management	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
10.	Clearing/Payment system	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
11	Foreign exchange trading	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
12	Litigation and legal matters	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
13	Human Resource	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
14	Foreign exchange trading	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No

6.2 RISK RATING

Risk weighting summarizes the risks inherent in the RSP's activities and the effectiveness of risk management in reducing those risks. It also summarizes the direction of those risks after considering internal and external factors that may affect the RSP's risk profile over time.

Steps in creating a risk rating include the following:

i. Identifying significant activities and functional areas
ii. Evaluating the quantity of inherent risks
iii. Evaluating the effectiveness of risk management
iv. Determining net (composite or residual) risk
v. Determining the overall risk rating, and
vi. Predicting the direction of risk

6.2.1 Identification of Substantial Activities/Functional Areas

Substantial activities include any substantial line of business, unit, or process. Substantial activities are identified from various sources, including RSP organization charts, strategic business plans, capital allocations, compliance with internal and external financial reporting, etc. For risk assessment, all identified common risks, namely liquidity, foreign exchange, interest rate, credit, reputation, operational including technology, compliance risk, and strategic risks, should be mapped onto such substantial activities to assist in identifying the risks inherent in each activity. See **Table 1**.

6.2.2 Determining the Quantity of Inherent Risks

The nature, complexity, and volume of RSP activities that give rise to given risks contribute to inherent risks. Inherent risks are associated with the nature, complexity, and volume of the activities that result in other specific risks. It is important to note that the assessment of inherent risk is made without considering management processes and controls, which are considered in evaluating the quality of the institution's risk management systems. Risk rating guidelines for assessing the quantity of inherent risk should follow the *Risk Management Guidelines for Remittance Service Providers*.[15]

Qualitative and quantitative criteria are used to assess the risks inherent in an RSP. For each category of risk (apart from operational risk), there are selected quantitative criteria in which benchmarks have to be established to determine the risk score of each criterion. These criteria originate from the *Risk Management Guidelines for Remittance Service Providers* and legal and regulatory provisions. All other judgmental criteria (mainly based on the *Risk Management Guidelines for Remittance Service Providers*) must be assessed to create a single risk score. The overall quantity of inherent risks will be determined using an average risk rating for each criterion. The levels of inherent risks can be low, average, substantial, and high, whose scores of 1, 2, 3 and 4 can be assigned, respectively. The four levels are defined as follows:

[15] The Risk Management Guidelines for Remittance Service Providers have also been separately developed by UNCDF

- **High inherent risk** exists when the probability of exposure leading to a substantial-to-high impact on an RSP's capital or earnings or liquidity or reputation, or operations is high. High inherent risk exists where the exposure is high, or positions are substantially large concerning the RSP's resources, where there is a large number of transactions, or where the nature of the activity is inherently more complex than normal. Consequently, the exposure or activity could result in a substantial and harmful loss to the RSP.

- **Substantial inherent risk** exists when the probability of an exposure leading to a high impact on an RSP's capital, earnings, liquidity, reputation, or operations is substantial. Substantial inherent risk exists where the exposure is significant. Positions are large concerning the RSP's resources, a significant number of transactions, or the nature of the activity is inherently more complex than normal. The exposure could result in a substantial loss to the RSP.

- **Average inherent risk** exists when the probability of exposure leading to a high impact on an RSP's capital or earnings is average. Average inherent risk exists where positions are moderate relative to the RSP's resources, the volume of transactions is average, and the activity is more typical or traditional. The exposure could potentially result in a loss to the RSP, which the RSP could absorb in the normal course of business.

- **Low inherent risk** exists when the probability of exposure leading to a high impact on an RSP's capital or earnings is low. Low inherent risk exists where the volume, size, or nature of the activity is such that even if internal controls have weaknesses, the risk of loss is remote, or, if a loss were to occur, it would have a little negative impact on the RSP's overall financial condition.

6.2.3 Assessing Risk Management Quality

When assessing the quality of an RSP's risk management, the primary consideration is reviewing a risk management system's following key elements:

a. Board of directors and management personnel supervision
b. Policies, procedures, and limits
c. Risk measurement, monitoring, and management information systems
d. Internal controls

A risk score will be assigned based on the judgmental assessment. The overall rating of the risk management quality will be determined using an average of the scores for the key elements. Risk management quality can be rated as strong, satisfactory, unsatisfactory, or weak, in which scores of 1, 2, 3 or 4 would be assigned, respectively. These ratings are defined as follows:

- **Strong risk management** indicates that management effectively identifies and controls all major risks inherent in the RSP. The board of directors and management personnel manage risks and ensure that appropriate policies and limits exist, and the board understands, reviews, and approves them. Policies and limits align with applicable laws and regulations and are supported by risk monitoring

procedures, reports, and management information systems that provide the necessary information and analyses to make timely and appropriate responses to changing conditions. Internal controls and audit procedures are appropriate to the size and activities of the RSP. There are few exceptions to the established policies and procedures, and none of these exceptions would likely lead to a significant loss to the RSP.

- **Satisfactory risk management** indicates that the RSP's risk management systems, although largely effective, may be lacking to some modest degree. Risk management systems are adequately in line with the requirements set by the nature of business. It reflects an ability to cope successfully with existing and foreseeable exposure from carrying out the RSP's business. While the RSP may have some risk management weaknesses, these problems have been recognized and are being addressed. Overall, the board of directors and management personnel supervision, policies and limits, risk monitoring procedures, reports, management information systems, and internal control systems are considered effective in maintaining a secure and protected RSP. Risks are generally controlled in a manner that does not require more than normal attention.

- **Unsatisfactory risk management** indicates that the RSP's risk management systems are not fully in line with the requirements set by the nature of the business. While the RSP has some risk management weaknesses, these problems have been recognized and are being addressed. The board of directors and management personnel supervision, policies and limits, risk monitoring procedures, reports, management information systems, and internal control systems are considered ineffective in maintaining a secure and protected RSP. Risks are generally controlled in a manner that does require more than normal attention.

- **Weak risk management** indicates that the RSP's risk management systems lack important aspects and are consequently a cause for concern. The system is considered not in line with the requirements set by the nature of the business. Unsatisfactory supervision by the board of directors and management personnel, policies, procedures, and limits, insufficient monitoring, and inadequate management information systems may all contribute to this. The internal control system may be deficient in key areas, as evidenced by ongoing control exceptions or a failure to follow established policies and procedures. If corrective efforts are not implemented promptly, the shortcomings related to these systems may jeopardize the RSP's protection and security.

Risk Management Guidelines for Remittance Service Providers can be a useful tool for assessing the risk management quality for each risk category.

6.2.4 Determining Net Risks

The net risk for each risk category is determined by balancing the quantity of inherent risks with the quality of risk management systems in the RSP. This is also known as composite or residual risk. The following table guides determining the net risk.

Table 2: Net Risks

DETERMINING COMPOSITE RISK RATINGS				
Quantity of Inherent Risks	Risk Management Quality			
	Strong	Satisfactory	Unsatisfactory	Weak
Low	Low	Average	Average	Substantial
Average	Average	Average	Substantial	Substantial
Substantial	Average	Substantial	Substantial	High
High	Substantial	Substantial	High	High

General definitions of the level of net risk for risk categories to facilitate consistency in the preparation of the risk matrix include the following:

- **A high net risk rating** would generally be assigned to an RSP where the risk management system is critically deficient in mitigating the high inherent risk. A weak risk management system could result in a high net risk where the inherent risk is substantial. This could be due to management personnel's insufficient understanding of the risk and capacity to anticipate and respond to changing conditions.

- **A substantial net risk rating** would generally be assigned to an RSP where the risk management systems do not substantially mitigate the inherent risk. For example, an RSP with low inherent risk but a weak risk management system could result in a substantial net risk. Likewise, an RSP with high inherent risk, despite having strong risk management systems, would result in a substantial net risk.

- **An average net risk rating** would generally be assigned to an RSP where the risk management systems mitigate the risks. Where there is a low inherent risk, unsatisfactory risk management systems may result in an average net risk assessment. On the other hand, a strong risk management system may reduce the risks of an inherently substantial risk activity so that any potential financial loss from the activity would have only an average negative impact on the financial condition of the RSP.

- **A low net risk rating** would generally be assigned to an RSP where inherent risk is low coupled with strong risk management systems.

6.2.5 Determining Risk Direction

The direction of risk adds a forward-looking perspective to risk management. In general, the direction of risk is forecast for the next twelve months and is a function of various factors, including the following:

a. Anticipated changes in the RSP's external environment
b. Planned changes in the strategic direction of an RSP, for example, new markets, products, systems, distribution channels, etc.
c. The current state of management and the related risk management systems.

The direction of risk can be increasing, decreasing, or stable.

Increasing risk indicates that other factors remain constant, i.e., an imbalance between the current or planned activities of an RSP and the underlying risk management systems. Specifically, the RSP's risk profile exceeds the ability of its systems to identify, measure, monitor, and control risk. Unless corrective action is implemented, RSPs experiencing increasing risks are exposed to greater losses that may adversely impact their financial position. The following factors can cause this imbalance:

- Changes in the external or competitive environment. For example, an increasingly competitive environment may cause strategic or other risk categories to increase even if an RSP has not initiated any internal changes.

- Opening branches or subsidiaries in new markets where money laundering is prevalent can cause ML/FT risks to increase.

- Increasing market volatility overall will cause an increase in liquidity, foreign exchange, and interest rate risks. While existing systems may have been adequate to support operations in a stable environment, they may be inadequate to compensate for the increase in market volatility and related loss exposures. A risk analyst would look to external data, such as news reports, industry and market trends, and the activities of RSPs within the market to judge whether an RSP faces increasing risk.

- The increasing risk may also result from internal factors, such as a change in strategy or business plans. A risk analyst will typically rely on off-site monitoring and the early warning system to identify increases in risk from internal factors. Situations of increasing risk are typically characterized by numerous instances of ratios either exceeding or lagging the peer and repeated flags in the early warning system. Additional warning signs indicative of increasing risk include the following:
  - Rapid growth in overall asset size or within a particular asset segment
  - Increasing concentrations of credit or funding sources
  - Unusually large positions in derivative instruments
  - Rapid initiation of new business activities

- Risks can also rise when the RSP's present risk management processes deteriorate. For example, to cut costs, management personnel may leave the scope of operations unchanged but reduce the risk management budget by half. Risks can also arise if management does not develop succession and training plans for management staff and cannot fill vacant risk management roles with qualified personnel.

Stable risk implies that the quality of the RSP's risk management systems is sufficient to balance and support the level of risk assumed. Note, however, that this does not require a static environment. For example, stable risk could be used to describe a situation in which:

- there have been no new entrants to the market;
- ownership structures have remained stable;
- few new products or innovations have been introduced;

- there is no indication of substantial changes in size, concentrations, or product mix;
- strategic plans and supporting budgets have remained the same, with relatively few changes in the staffing or resource levels supporting product lines; or
- all facets of the supporting risk management systems remain effective, including staffing composition and levels, reporting lines, and support functions.

Conversely, conditions within RSPs may have changed. Risk levels may have increased due to heightened competition, the introduction of new products, or growth. Nevertheless, RSPs may still exhibit a stable risk profile if risk management systems have been proportionately enhanced to compensate for the increased level of risk. For example, RSPs may have implemented a new product. By itself, introducing the new product increases the risk profile of the RSP. However, if management personnel have implemented appropriate risk-limiting mechanisms, including position limits, real-time monitoring, and effective separation duties, the overall risk profile of the RSP could still be regarded as stable.

Decreasing risk describes a situation where external factors become less influential or an RSP is streamlining or simplifying operations. Such situations include the following:

- An RSP exposed to fewer and/or less challenging competitors may be experiencing a decline in inherent risk.
- Periods of slow economic activity may also correspond to declining inherent risks.
- From an internal perspective, RSPs could reduce their exposure to risk by eliminating the use of complex strategies, products, or services. An RSP that concentrates on delivering products and services that are diversified and well-understood have a lower risk profile than an RSP that deals in, for instance, new complicated and poorly designed products and services. Consequently, the inherent risk may decline as an RSP moves from complex to simple strategies, products, or services.
- If an RSP closes its branches or subsidiaries previously located in markets susceptible to money laundering, the inherent risk may decline.
- Inherent risk can also decline if the RSP enhances risk management systems with no corresponding increase in risk profile. For example, implementing an effective internal audit function will reduce the level of operational risk in the RSP, with all other things remaining unchanged.

6.2.6 Determining the General Direction of Risks

The overall direction of risk will be determined by considering the quality of risk management systems, the direction of substantial risks affecting the RSP, and external and internal factors, for example, macroeconomic factors and the RSP's strategic plan.

6.2.7 Determining the Overall Risk

Once the net risk for each risk category has been determined, an overall risk assessment should be made for the RSP, the final step in developing the risk matrix. The overall risk rating is based on the weighted average of all net risk ratings, the weights being the risk significant factors determined judgmentally by the risk analyst. The direction of overall risk is also determined based on the judgment of the direction of each net risk.

'Weight' is determined according to the significance of the risk to the overall business profile of the RSP. It is important to remember that substantial risks pose a greater threat to the business failure or survival of the RSP (before considering the quantity of inherent risks and quality of risk management). The risk analyst will determine the 'weight' at an assessment stage. A cap of, for example, 30 percent and a floor of 5 percent weights (i.e., no single risk category will weight lower than 5 percent or higher than 30 percent) will be applied. It should be noted that high weights are assigned to risks highly important to the success or survival of the RSP and its business.

The weighted composite score for each risk category is determined by multiplying the composite score for each risk by its 'weight'. The overall risk rating will be determined as a simple summation of the weighted composite scores.

Determining the 'weight'of a given risk is part of the risk analyst's assessment of risks. It is a matter of professional judgment, based on the analyst's understanding of an RSP and, where necessary, in consultation with the other experienced personnel of the respective RSP. However, the following must be considered:

- An RSP's size, complexity, scope of activities, geographic diversity, and technology used
- An RSP's businesses, product lines, services, and functions
- Profiles and locations of substantial business units, departments, branches, subsidiaries, and products
- The nature of the operating environment (for example, changes in volume, economic and regulatory environment)
- Strategic plan, business plan, and strategies, including marketing emphasis, growth areas, acquisition or divestiture plans, and new products to be introduced

A sample of the risk matrix with assumed 'weights'weights is presented in Table 3 below.

Table 3: Sample Risk Matrix with Weights

Risk Category	Inherent Risk Scores	Quality of Risk Management Scores	Net Risk Scores	Weight	Weighted Net Risk Scores	Direction of Risk
Credit Risk	3 (Substantial)	2 (Satisfactory)	3 (Substantial)	20%	0.60	Increasing
Liquidity Risk	2 (Average)	1 (Strong)	1 (Low)	25%	0.25	Stable
Foreign exchange risk	3 (Substantial)	2 (Satisfactory)	3 (Substantial)	10%	0.30	Decreasing
Interest rate risk	3 (Substantial)	2 (Satisfactory)	3 (Substantial)	10%	0.30	Decreasing
Operational Risk			1 (Low)	30%	0.30	Stable
Reputational Risk			2 (Average)	5%	0.10	Stable
TOTAL				100%	2	
OVERALL RISK RATING & DIRECTION					AVERAGE	STABLE

6.2.8 Levels of Overall Risk Ratings

Overall risk rating for RSPs could have four levels, i.e., Low, Average, Substantial, and High. Each of these levels is described below.

- Low overall risk rating: an RSP has sound risk management practices, and its substantial risks are well managed. Weaknesses, if any, are minor and can be handled routinely by the board of directors and management personnel. An RSP with this rating exhibits the strongest performance and risk management practices relative to the RSP's size, complexity, and risk profile and gives no cause for concern.

- Average overall risk rating: an RSP has fundamentally sound risk management practices, and its substantial risks are well managed. Only average weaknesses are present and are well within the board of directors and management personnel's capabilities and willingness to correct them. Overall, risk management practices are satisfactory relative to the RSP's size, complexity, and risk profile. There are no material concerns.

- Substantial overall risk rating: an RSP has some degree of concern in its management practices, and its substantial risks are poorly managed. An RSP with this rating exhibits a combination of risk management weaknesses that may range from average to severe. Management personnel may lack the ability or willingness to effectively address weaknesses within appropriate timeframes. Risk management practices are less than satisfactory relative to the RSP's size, complexity, and risk profile. An RSP with this rating requires more than normal follow-up.

- High overall risk rating: an RSP has a high degree of concern in its risk management practices, and its substantial risks are inadequately managed. An RSP with this rating generally exhibits unsafe and unsound practices or conditions. There are serious managerial deficiencies that result in unsatisfactory performance. Risk management practices are generally unacceptable relative to the RSP's size, complexity, and risk profile. Close and ongoing attention is necessary, which means, in most cases, formal enforcement action is necessary to address the problems. An RSP with this rating poses a high risk, and failure is highly probable.

6.3 PRIORITIZATION OF SUPERVISORY ACTIVITIES

Once the overall risk rating for all RSPs is completed, prioritization can begin. Prioritization is done by looking at the RSPs' relative overall risk ratings, assessing possible impact on the market, determining the supervisory efforts needed, and coming up with a supervisory cycle based on the plan and available resources. The assessment of the impact involves estimating the potential harm to the market players that would result from the materialization of the risks. For example, the smaller the RSP the less the market impact should any risk materialize, thus the lower the ranking on the priority list, and the vice versa is true.

6.4 CONCLUSION

There are multiple frameworks and risk evaluation standards, each with its name and colour scheme. What is presented is one example of a risk management framework. Remembering that a risk rating system is a valuable tool for assessing and managing risk in various situations is critical. Moreover, risk rating is subject to legal system, nature of the market, data quality and availability, institutional setup, and supervisory experience within a particular jurisdiction. Regulators and supervisory authorities can methodically identify potential risks, assess their likelihood and potential impact, and guide RSPs to create effective mitigation plans by employing a structured approach and predetermined criteria. While risk cannot be completely eliminated, regulators and supervisory authorities could make better decisions and assist RSPs to reduce the possibility of unfavourable outcomes by using robust risk evaluation, weighting, and rating methodologies. As a result, it's crucial for regulators and supervisory authorities to periodically examine and update their risk assessment procedures and methodologies to make sure they continue to be useful in the face of changing circumstances and new risks.

ABOUT AFRICANENDA

AfricaNenda is an independent Africa-led organization created to accelerate the growth of instant and inclusive payment systems (IIPS) that will benefit all Africans, including the poorest and currently financially excluded. AfricaNenda's mission is to work towards universal access to inclusive payment systems ensuring that the more than 400 million unbanked adults across Africa are included in the financial system. The team aims to pursue this mission by removing the structural and technical barriers to effective deployment of IIPS such as lack of interoperability, insufficient technical in-house capacity, and minimal collaborative models across actors.

For more about AfricaNenda and the 2022 State of Instant and Inclusive Payment Systems in Africa findings, please visit: www.africanenda.org

ABOUT THE AFRICAN INSTITUTE FOR REMITTANCES

The African Institute for Remittances (AU-AIR) is a Specialized Technical Office of the African Union Commission. It was operationalized in 2015 with the core objective of developing the capacity of Member States of the African Union, remittance senders and recipients, and other stakeholders to design operational instruments and implement concrete strategies to use remittances as development tools for poverty reduction. Specific objectives include improvement of statistical measurement, compilation and reporting capabilities of Member States, promotion of appropriate legal and regulatory frameworks, and leveraging the potential impact of remittances for the social and economic development of Africa as well as the promotion of financial inclusion.

ABOUT IGAD

The Intergovernmental Authority on Development (IGAD) is one of the eight regional economic communities (RECs) and building blocks for the African Union. IGAD was established in 1996 to supersede the Intergovernmental Authority on Drought and Development (IGADD) which was founded in 1986. The new and revitalized IGAD was launched during the 5th Summit of IGAD Assembly of Heads of State and Government—Djibouti, Eritrea, Ethiopia, Kenya, Somalia, South Sudan, Sudan, and Uganda—held on 25-26 November 1996 in Djibouti. The Summit endorsed the decision to enhance regional cooperation in three priority areas of food security and environmental protection, economic cooperation, regional integration and social development peace and security. The founding leaders of IGAD were motivated by a vision where the people of the region would develop a regional identity, live in peace, and enjoy a safe environment alleviating poverty through appropriate and effective sustainable development programmes.

ABOUT ECCAS

The Economic Community of Central African States (ECCAS), created in 1983, comprises 11 Member States—Angola, Burundi, Cameroon, Central African Republic, Chad, Republic of the Congo, Democratic Republic of the Congo, Gabon, Equatorial Guinea, Rwanda, and São Tomé and Príncipe. It is one of the five development zones on which the African Union (AU) intends to build continental cooperation and integration.

According to its statutes, ECCAS' mission is to foster political dialogue in the region, establish a regional common market, set common sectoral policies, foster and strengthen harmonious cooperation, and balanced and self-sustaining development in all areas of economic and social activity, especially in the fields of industry, agriculture, natural resources, infrastructure, trade, customs, monetary and financial matters, and tourism.

ECCAS member states adopted a strategic plan for integration and a strategic vision in October 2007. The vision is to create by 2025 "a stable, prosperous, united, economically and politically united Central Africa" to make the region an area of peace, solidarity, and balanced development, with free movement of people, goods, and services.

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