African Union | AFRICAN INSTITUTE FOR REMITTANCES — Leveraging Remittances for Development | AfricaNenda — ACCELERATING INCLUSIVE PAYMENT SYSTEMS | IGAD | CEEAC-ECCAS | UNCDF

Risk management guidelines for remittance service 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, 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 the 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 these risk management guidelines was led by Albert Mkenda, remittance policy specialist, with invaluable inputs and support from Amani Itatiro, Doreen Ahimbisibwe, Mercy W Buku, and 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
CDD	customer due diligence
ECCAS	Economic Community of Central African States
e-KYC	electronic know your customer
FATF	Financial Action Task Force
ID	identification
IGAD	Intergovernmental Authority on Development
KYC	know your customer
ML/TF	money laundering/terrorist financing
RBA	risk-based approach
RSP	remittance service provider
UNCDF	United Nations Capital Development Fund

1.0 | INTRODUCTION

In the ordinary course of offering remittance services, a remittance service provider (RSP)[1] assumes risks inherent to the remittance business. While some are from the internal environment, others are from external environment. Assuming risk is necessary for the realization of returns on their investments. If not properly calculated and mitigated, the consequences of risks include negative impacts on the RSPs' goals, reputation, liquidity, and maybe even financial losses. These consequences may potentially reduce the customer base of RSPs and deplete their capital, hinder their operations, causing bankruptcy or cessation of business.

In offering remittance services, the risks could be either expected or unexpected. Expected risks are those that an RSP knows with reasonable certainty will occur, for example, the expected adverse movement of foreign exchange rates and inadequate liquidity in various currencies. Unexpected risks are those associated with unforeseen events, for example, losses due to a sudden economic downturn, natural disasters, or human actions such as terrorism.

Due to the risks facing the remittance business and their consequences, the need for effective risk management guidelines for RSPs cannot be over-emphasized. Through effective risk management, an RSP can implement robust policies to mitigate the risks and optimize their risk-return trade-off.

These guidelines have benefited from diagnosis reports[2] from extensive reviews and consultations in the Member States of regional economic communities (RECs) in Africa, where efforts are ongoing in collaboration with public authorities, particularly remittance services' policymakers, regulators, and supply-side stakeholders, to improve remittance policies that can lead to affordable, accessible, reliable, and tailored digital remittances and financial products to women and men migrants toward their economic inclusion, financial resilience, and reduced inequality. In this regard, the main objective of this work is to shed light on RSPs' efforts in improving existing and ongoing development of internal policies and risk management initiatives related to the remittance services they offer. The overarching objective is for the RSPs to put in place policies and risk management tools that will reduce or mitigate risks and therefore support the transition of remittance services from cash-based to digital channels and from informal to formal ones, ultimately leading to increased volumes and efficiency of remittance flows, lower costs, greater access, transparency, and financial resilience by migrants and their families.

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

[2] UNCDF, Research - Migrant Money (uncdf.org) (accessed on 17 February 2023).

2.0 | OBJECTIVE OF THE GUIDELINES

These guidelines aim to guide RSPs in identifying, evaluating, monitoring, and controlling key risks from the remittance services. A key component is risk management guidelines or rules that can guide RSPs in making decisions that would enhance risk identification and management practices. Moreover, the risk management guidelines can help to strengthen RSPs' capacities in developing, applying, and monitoring risk-based remittance policies and regulations to enhance market competition and innovation while safeguarding against risks to financial stability.

3.0 | RISK MANAGEMENT CONTEXT

Risk management includes all practices in identifying, assessing, mitigating, monitoring, and controlling the risks facing an RSP. Materialized risks can be costly, disrupt the remittance flows, hinder digitization, and perpetrate unregulated remittance channels. Therefore, effective risk management for the remittance market is in line with encouraging key players to the remittance channels to address the frictions causing the challenges of high cost, limited speed, transparency, and access. A risk-based approach (RBA) in conducting remittance business increases RSPs' ability to improve digitization, leading to improved usage and access to remittance services because a risk-based approach enables resource optimization by focusing resources on the most significant risks.

An initial risk management stage is locating or identifying possible risks, including gender-specific ones. This entails analysing all potential risks that might affect the goals, processes, or reputation.

The second stage is to evaluate the possibility and potential consequences of risks that have been identified. This entails assessing the likelihood that a risk may materialize and how it might affect the remittance services if it does. Where possible, the potential impact of risks on gender must also be assessed.

A third stage is to reduce the impacts of risks by employing risk mitigation measures taking into account gender aspects. This entails putting strategies and controls in place to lessen the chance and/or effect of the risks that have been identified, considering the specific needs of users of the remittance services, including women. Risks may be avoided, reduced, or accepted along with implementing management strategies.
Another risk management objective is monitoring, i.e., tracking how well the risk management plans and safeguards work. This entails routinely assessing the efficacy of the controls in place and continual examination and analysis of the risk management procedures.

All these activities aim to protect RSP's assets, minimize financial losses, ensure business continuity, and maintain stakeholders' trust by demonstrating that possible risks are being addressed methodically and proactively.

4.0 | REMITTANCE SERVICES CONTEXT

Migrant remittances are cross-border retail payments[3] that migrant workers send to their country of origin to support their families and pay for healthcare, education, and other costs. In this regard, remittances are a critical source of financing for people, particularly in developing countries, and play an important role in economic growth. Over the years, the remittance business has experienced enormous expansion, and so have RSPs. Remittance service providers include banks, money transfer companies, mobile money companies, and other fintech firms. The remittance business is regulated, with 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 pay directly for purchasing services, goods, or utility services in favour of their beneficiaries - payments to businesses and government agencies, i.e., person-to-business (P2B). Remittances can also be business-to-person (B2P), such as payment of insurance and pension to the 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).[4]

The challenges of sending remittances vary widely across country corridors,[5] types of RSPs, and gender of the customers, partly due to the different risk landscapes and types. For example, most international RSPs avoid conducting 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. Also, customers, particularly women, avoid using RSPs that they perceive as more susceptible to money loss, exploitation and abuse, or cultural and social barriers.

4.1 REMITTANCE SERVICE BUSINESS PROCESSES

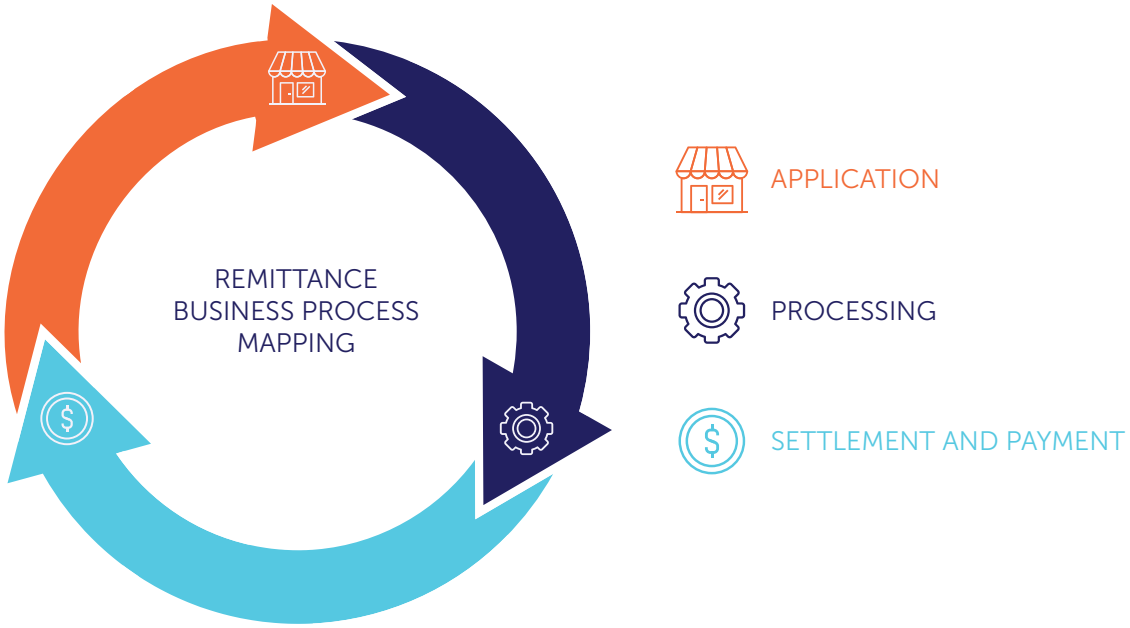
To better identify the risks facing an RSP, it is critical to map out all the business processes because most risks are either inherent to or originate from the RSP's business processes. The formal channels involve distinct processes from the application, processing of the application, settlement, and payment. Different RSPs have different instructions but generally follow the same process. A study of the remittance business processes is a starting point for identifying and mapping out all the risks linked to an RSP.

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

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

[5] The "country corridor" in this paper refers to money flows between two countries or regions.

Figure: Remittance Business Process Mapping



Remittance business processes are explained below.

a) **Application**

This is the fund capture phase, in which a person selects and contacts an originating RSP/electronic money provider and delivers funds to be transferred to a third party or distributed into a mobile wallet. The sender completes the registration, account creation, or sign-in processes and provides funds to be remitted or loaded in the electronic money wallet, including a fee and transaction information. The transaction information should include the sender/wallet holder and recipient's details[6] and the transaction amount. Validation would entail the originating RSP/electronic money provider performing checks as required by local AML/CFT regulations, gathering data on the relevant parties to the payment and confirming the transaction's legitimacy, liquidity availability, and other policy and regulatory compliance measures. Then, the RSP/electronic money provider checks the format and content of the payment message, verifies sufficient availability of funds, and transmits the transaction information.

Based on the anticipated delivery date and time specified, the sender can keep track of the fund transfer status.

[6] The details include name, address, and date of birth as would appear on a government-issued identity card such as a driver's license, passport, or national ID, etc. and/or banking details. Also, the details would include a pick-up location and currency of preference if the forex regulations permit.a

b) **Processing**

This is the transmission phase. Typically, the sender identifies the next recipient in the chain, transforms the data, and informs other parties about the payment status and the sender's details. The channel or designated location for picking up the money is also disclosed and indicated, along with the recipient's currency. However, it's essential to note that the possibility of receiving the money in the currency of choice depends on the recipient's country's forex regulations.

A unique transaction identifier is generated and transmitted if the money is not deposited in the recipient's account. The sender will provide the recipient with a unique transaction identifier. The payment message is then transmitted to the disbursing RSP or the recipient's electronic wallet.

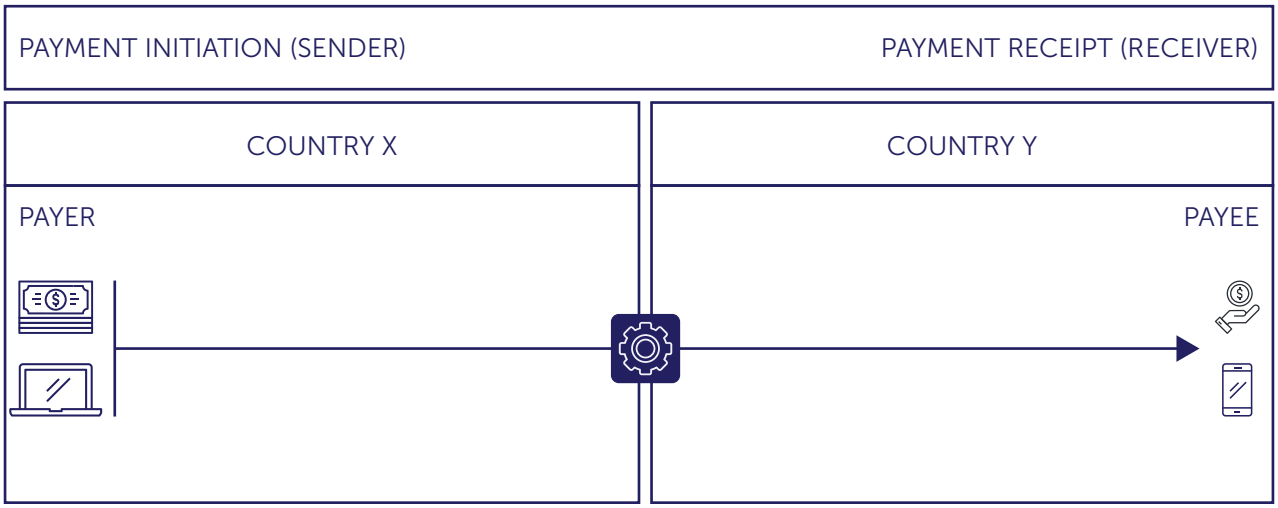
c) **Payment and Settlement**

This is the fund disbursement, communication, and settlement phase among the RSPs and involved agents. If the money is not deposited in the recipient's account or electronic wallet, the recipient of the funds will travel to the disbursing RSP and present the special transaction identifier. The transaction identifier is matched in the system, and if the identifier matches, the RSP approves the transaction. The disbursing agent releases funds after receiving the transaction approval. Subsequently, the originating RSP settles with the disbursing RSP. Depending on their contract terms, this could happen at the end of the transaction day or days later. At this stage, the originating RSP settles transactions involving different currencies across borders. Lags between fixing the exchange rate for the customer and undertaking the corresponding foreign exchange transactions create risks for participants, which can either be hedged or assumed on their own trading accounts. Compensation for that risk-bearing may be reflected in fees charged to customers.

4.2 MODE OF PAYMENT AND CHANNELS

The channels can also influence the risks facing RSPs in use and/or the mode of payment. Remittance payments can occur through decentralized arrangements, correspondent banking, centralized platforms, and interconnected platforms of RSPs in different countries.

a) **Decentralized Arrangements**

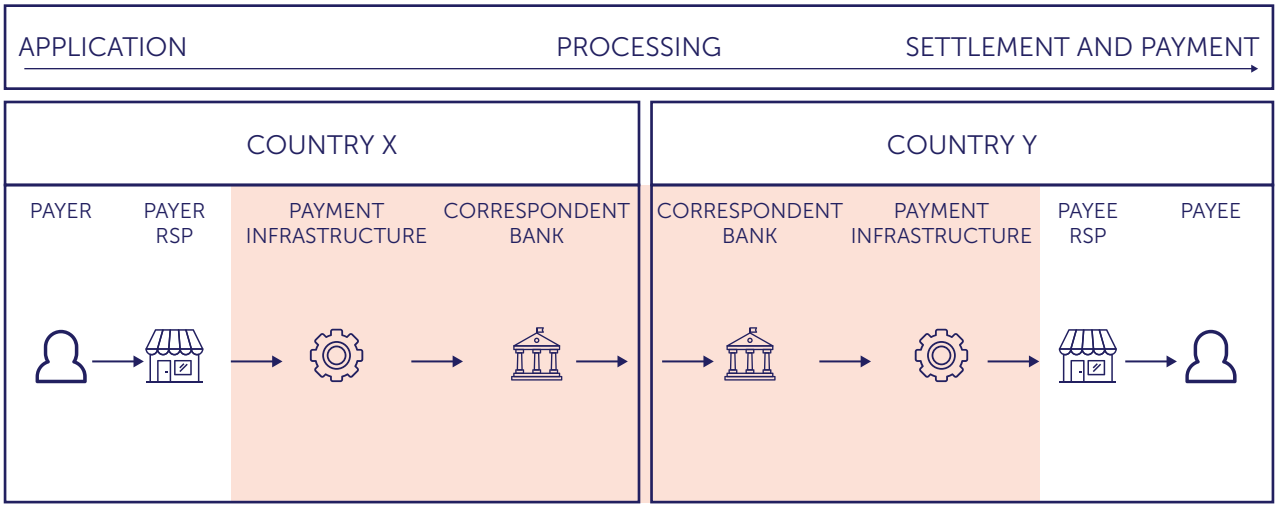


This mode of payment does not need an RSP. The payer sends money directly to the recipient.

Examples of decentralized arrangements are direct cash payment and the hawala system. Direct cash payment may, for example, involve physical money carried by an individual travelling between countries. The hawala system frequently relies on settling positions among a network of brokers rather than necessarily implying the actual movement of funds between intermediaries. Another example under the decentralized arrangement is the use of digital payment through distributed ledger technologies that can allow transactions to be executed electronically between parties using a shared ledger structure where the transaction is settled, and holdings are recorded.

b) **Correspondent Banking**

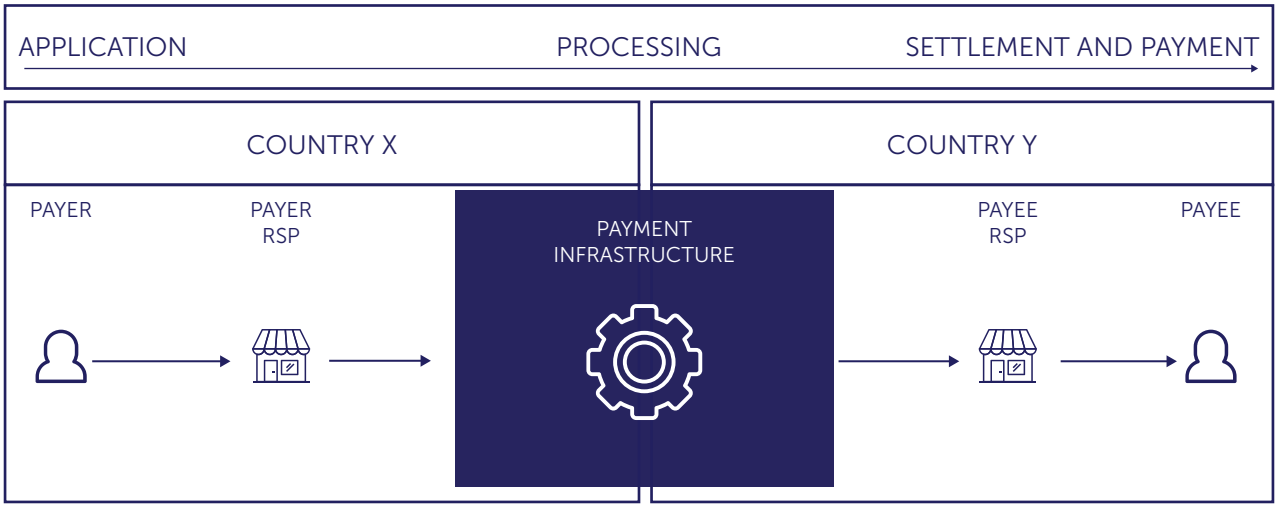
Correspondent banking refers to a financial arrangement that allows one RSP to offer services to another not in the same country.



In this mode of payment, a (correspondent) bank keeps deposits owned by other (respondent) banks from different countries while providing payment and other services to the respondent banks. Correspondent banking allows RSPs to access and offer cross-border payment services to their customers.

c) **Centralized Payment Infrastructures**

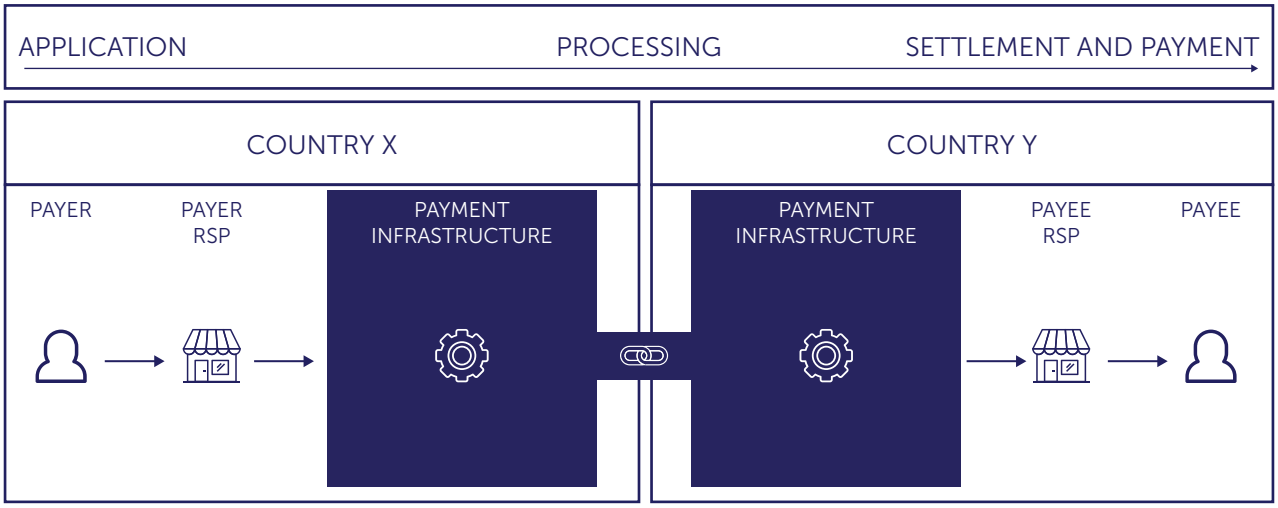
This can be an intragroup transfer where the RSPs of the sender and recipient are the same entity or members of the same group.



In this instance, the payment transaction bridges the two jurisdictions by initiating and concluding with the same RSP. As a result, it does not rely on a connection between RSPs or infrastructures in the two jurisdictions. This can be the case with franchised money transfer companies, some international card schemes, e-money schemes, or multinational RSPs operating in both sender and recipient countries.

d) **Interconnected Payment Infrastructures**

RSPs that are a part of one country's payment infrastructure can send and receive money to/from RSPs that are part of another country's payment infrastructure.



The interconnection can occur within a geographical region, such as links between automated clearing houses (ACHs) in the East African Community, i.e., the East African Payment System, or it can take place by arrangements between domestic infrastructures from various nations, such as the Pan-African Payment and Settlement System (PAPSS).[7] This arrangement comprises features to support currency exchange transactions when the payment infrastructures use different currencies.

The channels mentioned above 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.

4.3 RSP MODES OF PAYMENT AND CHANNELS AS SOURCES OF RISKS

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

Payment Systems

Payment systems are accustomed to conducting transactions. Moreover, multi-currency 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,[8] although bilateral settlement agreements are also available. Typically, these systems employ various messaging protocols. For example, some arrangements rely on proprietary messaging formats, one of the sources of operational risks.

Legal Frameworks

In these payment arrangements, legal risks come into play. Relevant legal and regulatory frameworks are required for the payment agreements or schemes to be entered into and become effective to enable processing, clearing, and settling cross-border payments. Typically, RSPs may enter into a bilateral or multilateral agreement, including operational and commercial rules and agreed-upon technical standards that participating RSPs agree to abide by. Additionally, RSPs' cross-border transactions are governed by several countries' policies and legal and regulatory frameworks, including consumer protection, cybersecurity, licensing and authorization requirements, prudential supervision and risk management, and AML/CFT frameworks. Most often, the regulatory frameworks may differ on transaction thresholds, the categories of entities permitted to conduct cross-border payments, and the licensing conditions, capital checks, and sanction laws. RSPs may, consequently, encounter challenges in locating comprehensive information on the nature of compliance requirements and become vulnerable to the interpretation and application of policy, legal and regulatory frameworks.

---

[7] PAPSS is a payment system designed to accelerate cross-border payments in Africa. As of the end of December 2022, 22 commercial banks – many with a pan-African reach – and six payment switches had signed up to the system.

[8] A settlement process that makes sure the final transfer of a payment in one currency only happens after the final transfer of a payment in another currency or currencies has already happened.

Payment Instruments

Payment instruments used can also influence the risk profile of an RSP. Senders and recipients of remittances can use various payment methods, including cash, e-money such as mobile money, credit cards, and electronic fund transfers. The instrument used depends on the RSP, the jurisdictions or regions involved in the transaction, and the type of end-users in question. For example, physical cash may be prevalent in areas where access to finance is low but increases the risk of money laundering. In Africa, for example, mobile money operations are prevalent. Technology risks increase with the use of e-money, etc.

As discussed above, all risks manifest in the remittance business processes and modes/channels of payment can be methodically categorized and defined for easy identification, assessment, mitigation, monitoring and control, and communication.

5.0 | KEY RISK CATEGORIES FACING REMITTANCE SERVICE PROVIDERS

The relatively small values involved in remittance transfers mean that it is unlikely for an RSP to pose systemic risk. However, at an individual level, an RSP does face liquidity, foreign exchange, interest rate, and reputational risks. Additional operational risk factors RSPs can face come from human actions, technological deficiencies, market operations lacking adequate transparency, and weak legal and regulatory frameworks. The following are key risk categories that RSPs may face in a given market.

5.1 LIQUIDITY RISK

This is an RSP's exposure resulting from its inability to satisfy its obligations when they become due or from its failure to fund asset growth without incurring unacceptable expenses or losses. Liquidity risk includes exposures from the inability to manage unplanned decreases or changes in funding sources. If an RSP fails to meet its obligations, it must often depend 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,[9] custodian banks, liquidity providers, and associated payment infrastructures to perform as planned can create liquidity risks.

In general, liquidity risk factors include one or a combination of the following:

i. Arrangements to pay the recipient before the funds from the sender arrive.
ii. The need to hold funds to enable rapid onward settlement, often across multiple currencies, brings in an opportunity cost of being unable to invest funds.
iii. Uncertainty over when incoming funds will be received may lead to overfunding positions and increased costs. Funding costs are typically higher for transactions in illiquid or non-tradeable currencies.
iv. Poor access to foreign currency markets.
v. Failure to recognize or address changes in market conditions that affect the ability to liquidate assets quickly and with minimal loss in value.

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

vi. The slow speed of cross-border transfers causes delays and increased liquidity risk.
vii. Liquidity facilities access limitations. A non-bank RSP can hardly access liquidity facilities through interbank markets or the central bank as a lender of last resort. In addition, a smaller RSP may need to rely on bigger banks in foreign jurisdictions, with additional costs.

Borrowing funds to provide liquidity is costly. RSPs must ensure they have enough liquid assets to meet their customers' eligible demands and complete transactions with their correspondents. Transactions delayed or cancelled due to a lack of liquidity may harm an RSP's reputation and customer trust.
In principle, liquidity risk should not be seen in isolation. Consequences of other financial risks, such as credit, interest rate, and foreign exchange, often create liquidity risks because financial risks are not mutually exclusive.

5.2 FOREIGN EXCHANGE RISK

Remittance transfers frequently involve foreign exchange transactions. Foreign exchange risk factors include one or a combination of the following:

i. Cross-border processing of payments from a sender in its local currency to the recipient in its local currency raises foreign exchange considerations.
ii. The exchange rates fluctuate from time to time due to various factors in the financial markets. An RSP 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.
iii. Additionally, foreign exchange risk factors include processing speed, i.e., when processing speed is low, the cost of foreign exchange settlement risks increase.
iv. 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. RSPs must manage these risk factors through hedging strategies and deploying proper risk management guidelines.

5.3 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.

Interest rate risk factors include one or a combination of the following:

i. Unfavourable movements of interest rates
ii. Adverse movements of prices in the market affecting the cost of operations and remittance fees

Changes in interest rates can also affect the profitability of transactions. RSPs must manage these risk factors by deploying proper risk management guidelines.

5.4 CREDIT RISK

Credit risk arises from the exposure of 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 chain transactions do not occur in sequence, the receiving agent may disburse funds to the final beneficiary customer upon receipt of the payment message but before the sending RSP transfers the money. A transmitting RSP might agree with the disbursing agent that liquidity will be made available for the agent to pay the recipient as soon as the message is received or at a specific time afterwards. The "paying before being paid" situation makes an RSP run the risk of losing money, in which case the disbursing RSP takes on credit risk.

Broadly, credit risk factors include one or a combination of the following:

i. For franchised RSPs,[10] the recipient occasionally chooses 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. If there is no liquidity agreement between them, the disbursing agent may be exposed to credit risks.
ii. Another source of credit risk exposure is the possibility that an RSP provides services in addition to remittances, such as banks. They may accept payments and extend credit in the normal course of business.
iii. Low speed of cross-border payments may cause delays and increase credit risk.
iv. Pre-settlement risk, i.e., the possibility of losing unrealized gains on transactions with a counterparty that have not yet been settled. The cost of reconducting the first transaction at current market values constitutes the potential loss that could result.
v. Settlement risk, i.e., the possibility that a counterparty will lose the full value involved in a transaction. For example, there is a possibility that an RSP will deliver the service irrevocably but not get paid for it.
vi. Reliance on other banks in foreign jurisdictions, with accompanying additional credit risk.
vii. Extension of credit facilities by an RSP to its agents and/or customers.
viii. Other potential sources of credit risk include the inability of settlement banks, custodians, or payment infrastructure operators to fulfil their financial commitments.

5.5 OPERATIONAL RISK

Operational risk is exposure from inadequate or failed RSP's internal processes, people, and systems that can lead to limited, deteriorated, or the breakdown of services causing losses or the decline of earnings and capital. Other sources of operational risk include eternal events and operational flaws, which can lessen the impact of management personnel actions on other risks. Both internal and external factors can contribute to operational risk. Processing mistakes or delays, lack of proper documentation, poor management, lack of or inadequate contingent plans, inadequate policies, procedures, and controls,

[10] A franchised service is where a central provider, creates infrastructure to support the remittance service but obtains the necessary access points by inviting institutions in both sending and receiving countries to offer the service or act as franchisees on standardized terms.

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 an external factor is when participants in a payment system, for instance, expose other participants to operational risks, which may lead to liquidity issues or other operational problems for them.

These internal and external exposures may cause technology breakdowns, cyber-crimes, poor contracting, poor contract enforcement, disproportionate and discriminatory licensing procedures, disproportionate prudential supervision, poor financial integrity, ineffective risk management practices, inadequate customer protection, and disproportionate forex regimes. In addition, operational risks such as money laundering/financing of terrorism (ML/FT) risks[11] may be inherently higher because remittance services involve non-face-to-face business relationships or transactions.

All these operational 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.

As detailed hereafter, the operational risk may be re-categorized into four sub-categories - compliance (legal), strategic, country (political), and technological.

5.5.1 Compliance Risk

The possibility that legal action will be taken against an RSP because of its actions, inactions, products, services, or other events. These can bring in the possibility of potential non-compliance with legal and regulatory frameworks. Disjointed regulatory frameworks may increase the exposure to this risk. Actions or inactions leading to omission may result in regulatory penalties and sanctions.

An RSP is usually subject to various compliance requirements, such as 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.

This risk category includes the legal risk, i.e., misinterpretations of the 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 risks 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.

One of the following risk factors could expose an RSP to compliance risks:

i. Breaking or failing to abide by the laws, rules, agreements, specified procedures, or ethical standards.

[11] Given the importance of the ML/FT risk in remittances, a separate guide has been issued specifically to cater to this risk category. See links: RSP AML_CFT Guidelines.docx and RBA Guide.docx

ii. Improper application of rules and/or legislation.

iii. Legal actions taken against an RSP.

iv. Claims made by customers due to poor service, delays, loss of service, or damage involving the RSP's operations, personnel, or services.

v. Inability to handle relationships with a sizable number of stakeholders, including tax authorities, local authorities, and other authorized agencies, as well as regulators, customers, counterparties, and customers.

vi. An inadequate understanding of an RSP's and its customers' rights and obligations.

vii. Making improper use of the remittance service, such as for money laundering.

viii. Insufficient plans that would guarantee that recipients receive their payments on time even if there has been a loss in transit.

ix. Inadequate adherence to the requirements for transparency to prevent money laundering and the financing of terrorism and proliferation in cross-border payments.

x. Expensive screening procedures, including compliance checks, when a transaction passes through the payment chain.

xi. The data may be inaccurate when deploying different sanction lists and other databases to carry out checks, e.g., false positives where entities have names that have a similar spelling to names on lists.

xii. Maintaining the minimum statutory capital requirements may be expensive.

xiii. The need for additional human resources to comply with other supervisory criteria, such as submitting returns, reserves requirements, insurance requirements, premises specifications, technology specifications, etc.

xiv. Non-compliance with the legal and regulatory frameworks governing foreign exchange, particularly when the market is volatile, or the forex system is rigid, leading to parallel markets.

xv. Lack of adequate skills and knowledge, inadequate training, improperly aligned compensation schemes, lack of understanding of performance standards or expectations, and inadequate human resource supervision and segregation of duties. These may further lead to the following risk factors:
    - Data entry errors due to human errors
    - Fraud such as intentional misreporting of positions, employee theft, robbery, forgery, and damage from computer hacking

- Weaker implementation of AML/CFT standards may, in turn, prevent efforts by correspondents and other institutions in the payment chain to ensure illicit finance and terrorist financing risks are appropriately assessed and mitigated. This may further lead to de-risking
- Internal and external system security issues
- Legal issues

Compliance risks can result in license revocation, financial penalties, damage payouts, a decline in market share, and a restricted capacity for expansion. Compliance risks can also result in reputational risks, hindering 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.

5.5.2 Country Risk

The exposure that could occur to an RSP when conducting business in a foreign jurisdiction is called 'country risk.' Such risks can also arise from conducting business or lending or borrowing money internationally. Political, legal, and regulatory aspects that vary between regions or countries may also pose country risks. RSPs may be exposed to 'country risks' simply because of their operations in other nations where there may be high-risk locations, for example, money laundering and terrorism funding.

RSPs may be subject to country risk exposures due to one or more of the following factors:

i. Operations in markets with inadequate transparency and weak legal and regulatory frameworks
ii. Borrowing or lending abroad
iii. Disparate legal, regulatory, or political systems in various nations or regions
iv. Domestic political changes or unrest
v. A change in the country's executive, judicial, legislative, or military branches
vi. Government decisions and announcements impacting specific RSPs and the national economy. For example, announcements relating to taxes, spending, rules, currency valuation, trade tariffs, and labour laws such as minimum wages
vii. Terrorism
viii. Vandalism
ix. Earthquakes
x. Fires
xi. Floods; and
xii. Wars

5.5.3 Technological Risk

Technology-related failures or other occurrences that may harm remittance services, people, other RSPs in the market, or society at large are referred to as technological risks. One or more of the following factors could expose an RSP to technological risk:

i. Interdependencies of payment infrastructure can transmit disruptions beyond a specific RSP and its participants and affect other RSPs.
ii. An event hampering the payment systems can lead to the inability of an RSP to fulfil some or all its business obligations, particularly where the RSP's physical, telecommunication, or information technology infrastructures have been damaged or made inaccessible.
iii. Challenges to accessing payment systems and services. RSPs may not be able to directly access local and foreign payment systems and possible funding in foreign currencies. This may make it dependent on other providers and may inherit the latter's services, cost, and AML/CFT policies, consequently impacting their cross-border payment offerings.
iv. The complexity of reconciliation processes is due to variations in data standards and formats across jurisdictions, payment infrastructures, and message networks. This may create processing costs and delays.
v. Damaged physical assets relating to the information systems used by an RSP and inadequate or obsolete technology.
vi. Software failures.
vii. Telecommunication problems.
viii. Utility outages.
ix. Legacy systems, i.e., simply automating the old manual method to introduce a payment processing system, can potentially prolong the risks inherent in manual processing.
x. System limitations, such as a reliance on batch processing, a lack of real-time monitoring, and low data processing capacity, may also lead to delays in settlement and inefficiencies in liquidity management.
xi. System breakdowns and errors can occur in complex IT systems responsible for processing remittance transactions.
xii. Using unproven or unreliable hardware, software, or infrastructure.
xiii. Inefficient maintenance of the payment systems and infrastructures.
xiv. Human mistakes and/or misbehaviour.
xv. Cybersecurity breaches.
xvi. Cyber-attacks.
xvii. Improper IT project management.
xviii. Failure of critical systems, such as power grids or transportation networks, due to technical malfunctions or cyber-attacks.
xix. Hacking, etc.

These accidents may lead to data loss, equipment damage, and disruption of essential systems and services. Any of the above 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.

5.5.4 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 determined by 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, which can result in market share losses, reputational harm, and/or monetary losses. Examples of strategic issues include the following:

i. Failure to foresee or respond to changes in the business environment, such as customer preferences or economic instability.
ii. Internal elements such as poor management, a toxic internal culture, or insufficient funding may impact or prevent the strategic plan from being carried out. Such factors include an organizational structure that does not align with its plans and prevents conflicts of interest among its directors, managers, shareholders, and staff.
iii. Failure to engage in research and development to stay up with industry developments.
iv. Entering new markets without conducting adequate study and preparations.
v. Bad business judgments, poor execution of decisions or a lack of market response, and economic changes influence an RSP's earnings, capital, reputation, or good standing in the present and the future.
vi. External elements can impact or prevent achieving 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 elements include competition, shifting consumer markets, regional or national economic conditions, and alterations to laws and regulations.

5.6 REPUTATION RISK

The reputational risk refers to any potential 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 one or more of the following:

i. An RSP's failure to have sufficient plans to guarantee that recipients receive their funds on time even if there has been a loss in transit.
ii. Using the service illegally, e.g., for drug trafficking, human trafficking, or money laundering purposes.

6.0 | RISK MANAGEMENT GUIDELINES

This section is intended to help RSPs develop internal risk management guidelines. It is important to note that risk management guidelines must be subject to policy, legal and regulatory requirements governing RSP's operations in each market. It is important to note that the degree of formality and sophistication of an RSP's risk management framework should be commensurate with the RSP's size and risk profile.

6.1 GENERAL RISK MANAGEMENT GUIDELINES

The risks facing an RSP can be catastrophic and must be carefully managed to ensure the reliability, security, and profitability of its operations, leading to reliable and affordable remittance services to women and men migrants and their families. This requires a strong focus on compliance, operational resilience, liquidity management, credit risk management, foreign exchange risk management, interest risk management, and protecting the reputation of the RSP.

6.1.1 Environmental Scanning

Both external and internal risk factors should be well captured in developing risk management guidelines.

External Environment

The external risk factors must be scanned thoroughly, and respective risk management guidelines can be designed. The external environmental risk factors include the following:

i. **Competition**

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

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 women migrants. 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.

RSPs should ensure that factors such as these are well considered in developing effective risk management guidelines.

iii. **Technological Changes**

Due to changing technology, RSPs may fail to properly position themselves or perform well in the market. At the same time, its competitors can develop more efficient systems or services at lower costs. The RSP 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 operations and 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. **Government Policy and Regulations**

Changes in laws and regulations governing the financial sector, tax authorities, local authorities, and other regulatory agencies may affect the risk profile of an RSP and the implementation of its strategic and business plans. RSPs may need to adjust their reporting systems and plans to ensure compliance. Effective risk management guidelines should take into account all these factors.

Internal Environment

Internal environmental risk factors must also be scanned thoroughly. They include the following:

i. Organizational Structure

In general, an organizational structure is important for implementing strategic and business plans and meeting overall goals in the most efficient manner. A poorly designed structure may pose substantial operational risks. In this regard, RSPs must establish clear organizational structures. The organizational structure of RSPs should be consistent with its plans and be able to reduce conflicts of interest among its shareholders, board of directors, management personnel,[12] and staff.

ii. Work Processes and Procedures

These enable the timely and accurate implementation of business plans. If not appropriately handled, they may expose an RSP to operational risks. The board of directors should establish responsibilities and clear guidelines, policies, and measures to avoid deficiencies in work processes and procedures.

iii. Information

With a rapid and timely flow of information, most risk exposures of an RSP can be minimized. On the contrary, a lack of adequate, relevant, accurate, and timely information exposes an RSP to various risks. A thorough understanding of the market has a favourable impact on creating business strategies and developing risk management guidelines.

iv. Technology

Technology systems are also sources of operational risk that RSPs may face. Technology systems should be able to handle the volume of transactions and all customer needs efficiently and effectively to maintain competition and develop new business lines. Risk management guidelines in respect of technology are also important.

v. Personnel

Knowledge, experience, and vision of the board of directors, management personnel, and staff are crucial for strategic and business plans' success. RSPs should demonstrate a knowledgeable board of directors, competent management personnel, and staff with relevant experience in managing the risks they may face. RSP's personnel are a source of many risks facing it. RSPs must implement risk management guidelines delineating lines of authority and responsibility for managing each risk category.[13] A lack of qualified and sufficient staff can lead to increased risk exposures, poor financial results, and reputational harm for the RSP.

It is also important to ensure diversity, including gender, on the boards, staff, and management.

---

[12] Management personnel 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.

[13] Risk category refers to the (i) liquidity risk, (ii) foreign exchange risk, (iii) interest rate risk, (iv) credit risk, (v) operational risk, and (vi) reputational risk.

Board of Directors or its Equivalent

Understanding the risk category and degree of exposure ultimately rests on the board of directors.

Specifically, the board of RSPs should be responsible for the following:

a. Developing a strategic plan for the remittance business and each new product.
b. Approving each risk category's management policy, setting clear rules and principles for managing the risk and creating a management structure, and carrying out the RSP's risk management process. The board should periodically review the RSP's risk management policy to ensure the right guidance is provided.
c. Being familiar with an RSP's profile and the necessary instruments for managing each risk and ensuring the availability of adequate personnel and infrastructure required to manage the risk in all relevant scenarios.
d. Ensuring the presence of qualified individuals with the necessary motivation to perform their duties. Often, non-executive board members must be included, and considerations on gender should be made.
e. Clearly defining roles, responsibilities, and processes for its operation, including identifying, handling, and resolving board member conflicts of interest.
f. Routinely evaluating its overall performance and the performance of each board member.
g. Ensuring that the design, rules, overall strategy, and major decisions appropriately reflect the legitimate interests of its direct and indirect stakeholders. In this regard, the board should regularly review the risk management guidelines to ensure the RSP manages the risks from external markets and those associated with new products, activities, or systems. This review process should also assess industry best practices in risk management appropriate for the RSP's activities, systems, and processes. Major decisions should be disclosed to relevant stakeholders.
h. Establishing a clear, written risk management structure specifying roles and accountability for decisions, incorporating the RSP's risk-tolerance policy and addressing crisis and emergency decision-making. The board must establish distinct lines of management responsibility, accountability, and reporting since establishing robust internal controls is crucial to managing risk. Risk control, business lines, and support functions should have distinct roles and reporting structures to prevent conflicts of interest.
i. Adopting a strategy and policy for each risk category and ensuring the RSP management personnel takes the appropriate measures to identify, assess, quantify, monitor, and control each risk.
j. Ensuring reliable risk management procedures are properly detailed in the respective risk strategy and policy. The board must communicate the strategy's guiding ideas to the RSP management personnel and give its consent to any relevant developed policies.
k. Monitoring changes in the market and technological developments to keep RSPs competitive and enable quick responses to customer requirements.
l. Reviewing the management personnel performance against set goals at least annually.
m. Designing a procedure or strategy for management personnel transition.
n. Giving the management personnel specific directions regarding their duties in risk management and ensuring that the management personnel and staff are responsible for implementing the RSP's risk

management systems and that an efficient and thorough internal audit function is responsible for reviewing it.

o. Endorsing broad business objectives and directives that control or affect each of the RSP's risk categories and ensuring that clear instructions are provided to the RSP management personnel outlining the reasonable level of each risk that the RSP can endure.
p. Approving any internal policy outlining who oversees what and how much when managing exposure to each risk.
q. Routinely assessing and reevaluating the general business strategy that affects an RSP's exposure to each risk category and the associated risk management procedures.

Management Personnel

RSP management personnel should be responsible for the following:

a. Having essential knowledge of each risk category and being 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 board-approved policy.
b. Possessing the ability and moral character to carry out their duties concerning risk management and managing effective internal controls and ethical standards.
c. Translating the risk management guidelines for each risk category into concrete policies, processes, and procedures that can be applied and verified within the various business units. Management personnel should delineate who has what power, responsibility, and reporting connections to encourage and sustain this accountability. Furthermore, considering the risks associated with a business unit's policy, management personnel should evaluate the suitability of the oversight process and make sure that the necessary resources are available to manage each risk efficiently.
d. Putting the strategy and the policy into practice in a way that reduces the exposure associated with each risk category and assures adherence to the country's governing policies, rules, laws, and regulations. Moreover, the RSP management personnel should be responsible for developing and implementing internal policies and practices that translate the RSP's goals, objectives, and risk tolerance into operating standards that are well-understood by RSP personnel, as well as for the interest rate risk reporting and review process, effective internal controls, and ethical standards.
e. Overseeing the implementation and maintenance of management information and other systems for each risk category that identifies, measures, monitors, and controls their respective risks.
f. Assessing the sensitivity of an RSP to changes in market conditions and other substantial risk factors by using aggregated information and supporting data provided in the risk assessment reports.
g. Prioritizing the operational risk management goals based on their strategic importance to translate the strategic goals into attainable objectives. Within the general structure of an RSP, strategic goals should be broken down into smaller, more manageable actionable chunks and assigned to various business units. Plans and objectives should align with the nature, scope, and complexity of the RSP's activities and the market in which those activities are conducted.
h. Taking charge of managing and overseeing an RSP's overall risk environment daily.
i. Establishing reasonable limits on taking risks, creating criteria for assessing job performance, and creating standards for valuing positions related to each risk category.

j. Ensuring that the RSP's activities are carried out by qualified staff with the requisite authority, experience, technical know-how, and access to requisite resources. The reward rules must align with risk tolerance because positive rewards for personnel who violate policies may erode the effectiveness of the RSP's risk management procedures.
k. Ensuring adequate technological and human resources are allocated to managing each risk category and ensuring that all business lines receive regular compliance training that addresses compliance obligations, especially when entering new markets or introducing new services.
l. Informing all relevant people of the policies, processes, and procedures.

Other Staff

a. A specific, named individual or committee within an RSP with the necessary skills and a thorough understanding of a risk category's nature, magnitude, and management may oversee that risk category facing an RSP.
b. The staff responsible for each risk category must have the qualifications and skills to evaluate and control the relevant risks 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.
c. Personnel working on the validation process should be autonomous from the implementation and model development activities.
d. All staff members should know internal controls for managing each risk category. Staff members are required to follow the established lines of authority and responsibility.
e. At both the transactional and portfolio levels, responsible staff should be able to identify and quantify the main sources of risks quickly and reliably.
f. Close connections between those in charge of each risk category, those keeping track of market circumstances, and others with access to vital information are required.
g. A timely flow of information among the front office, back office, and middle office in an integrated manner is critical while ensuring their reporting lines are kept separate to ensure the independence of these functions.
h. The scope of the compliance function and its personnel requirements (number and competencies) is determined by the size of an RSP and the complexity of its business operations. A compliance unit does not always handle all compliance-related duties. Employees from specific departments may carry out the compliance duties specific to that department, or the compliance unit/department may handle overall compliance duties.

6.1.2 Risk Management Tools

These tools include a strategic plan, a risk management policy, and an operations manual.

Strategic Plan

a. For day-to-day management, RSPs should have a predetermined strategy for each risk category. The strategic plan should outline the overall approach to managing each risk category and numerous quantitative and qualitative goals. This strategic plan should outline how to safeguard the financial stability of the RSP and endure adverse market circumstances.

b. The strategic plan should be formulated after determining the RSP's appetite for each risk category and should strike a balance between the corporate objectives and that appetite.
c. RSPs should consider the influence of economic conditions while formulating a strategic plan, considering whether the RSP possesses the knowledge necessary to profit from a particular situation and the ability to recognize, track, and manage the risk associated with each situation and transaction. The strategic plan should consider constructing a portfolio mix to protect the RSP from increased risk.
d. The strategic plan should provide for managing outsourcing agreements' performance and establishing remuneration policies for management personnel and staff. The remuneration should be commensurate with the RSP's financial situation.
e. The strategic plan should align with the organizational structure and job descriptions and address each position's essential requirements and capacity-building requirements.
f. The board should endorse and evaluate the strategic plan at least once a year.

Risk Management Policy

a. RSPs should create a policy for each risk category to implement the strategic plan. The procedures for implementing the policy should be followed at all levels of the RSP and should be communicated in a timely manner. Any violation of the policy provisions must be reported, and appropriate action must be taken. Consolidated and, if necessary, certain subsidiaries, agents, affiliates, or units within RSPs should be subject to the policy.
b. The policy should specify how each risk category is identified and measured, how to decide the respective risk appetite for the RSP, how often risk limits are reviewed, and how each risk is evaluated.
c. The policy should specify the roles and responsibilities of the board of directors, management personnel, and other individuals managing each risk category. The policies should also specify the structure of each risk limit, the delegation of approving authority for each risk limit and limit excesses, capital requirements, and the investigation and resolution of erroneous or disputed transactions, in addition to providing guidelines on all these topics.
d. An RSP's risk management policy and processes should be frequently evaluated to ensure they are still acceptable and solid. The policy on each risk category is anticipated to be reviewed at least once a year, except for unusual situations.
e. An RSP personnel must be informed about the policy and any changes that may be made from time to time in response to changing economic conditions and other factors.
f. The policy on each risk category must be distributed throughout the RSP.

Operations Manual

RSPs should create an operation manual for each risk category to implement each policy. The manual should set up detailed protocols, processes, and constraints. The manual must be reviewed and updated regularly to reflect new projects and developments and to update risk management strategies and procedures as needed.

6.2 SPECIFIC RISK MANAGEMENT GUIDELINES

Sound governance and risk management guidelines for each risk category on the part of an RSP are critical to avoiding or reducing the impacts of the risks. The risk management policies, procedures, and systems should assist an RSP 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.

Interdependence exists in remittance markets. Consequently, RSPs should further assess the significant risks it faces and exposes to other RSPs, settlement banks, and liquidity providers and develop the requisite risk management systems to mitigate the risks. The effectiveness of a wide range of recovery or exit options should be evaluated, and RSPs should identify circumstances that could potentially preclude it from being able to perform its essential operations and services as a going concern.

6.2.1 Liquidity Risk Management Guidelines

RSPs should generally have liquidity provisions that allow them to pay the recipients before the sender's money has arrived. Negative credit, capital, or reputation trends can substantially impact the RSP's liquidity. A decline in the RSP's financial health could lead to reduced funding availability. The nature, scale, and complexity of the RSP's activities should be reflected in the formality and sophistication of the risk management systems developed to control liquidity risk.

An RSP must implement mitigation controls and be aware of the variables that could result in liquidity risk. The default of other participants and their affiliates should be included in addition to other potential stress scenarios. RSPs should also keep additional financial resources sufficient to address these scenarios.

The formality and sophistication of an RSP's liquidity risk management framework should be commensurate with the RSP's size and risk profile.

Liquidity Risk Assessment, Monitoring and Control

a. RSPs should efficiently assess, monitor, and control their liquidity risk and maintain enough liquid assets in all relevant currencies. They should also establish a guarantee fund to confidently execute same-day, real-time settlement of payment obligations under various potential stress scenarios. Following individual or collective participants' default, RSPs should create clear rules and procedures to execute same-day and/or real-time settlement of payment obligations. The goal is to prevent the unwinding, revocation, or postponement of the same-day settlement of payment commitments and to handle unexpected and possibly hidden liquidity deficits. For the RSP to continue operating securely and reliably during a stressful event, these rules and procedures should also outline the RSP's strategy for replenishing any liquidity resources it may use during a stressful event. This calls for efficient operational and analytical tools to recognize, quantify, and keep track of the funding and settlement flows regularly. In all circumstances, the RSP should have a written justification for the level and type of total liquid assets it keeps and suitable governance procedures in place.
b. RSPs should complete final settlements no later than the end of the value date, preferably in real-time, to reduce settlement risks. The RSP should clearly define the point after which a participant may not revoke unsettled payments, transfer instructions, or other obligations.

c. A comprehensive structure for managing liquidity risks from participants, settlement banks, nostro agents, custodian banks, liquidity providers, and other entities should be in place.
d. The liquidity strategy should specify the asset and liability mix needed to preserve liquidity. Asset and liability management should be integrated with liquidity risk management to reduce the high costs of a sudden change in the asset-liability profile from maximum profitability to greater liquidity. The strategy should explain how diversification and stability of obligations may be achieved under different circumstances, such as when money is suddenly and substantially withdrawn, which could increase liquidity risk.
e. A liquidity management policy (short- and long-term) should contain specific goals and objectives for managing liquidity risks, the method for formulating liquidity plans, and the level at which it is accepted within an RSP. The policy should also include the roles and duties of people conducting structural balance sheet management, pricing, marketing, management reporting, lines of authority, and accountability for liquidity decisions. The policy should emphasize liquidity risk management tools for identifying, measuring, monitoring, and controlling liquidity risk (including the kinds of liquidity limits and ratios in place and the justification for establishing limits and ratios), as well as contingency plans for dealing with liquidity stressful events.
f. RSPs must manage liquidity across several currencies. The RSP should have a policy with clear provisions for handling liquidity in various currencies. The possibility of short-term and long-term liquidity disruptions, along with the associated costs, should also be addressed in the policy.
g. The provisions of the liquidity policy must be conveyed at all levels within the RSP.
h. RSPs should have reliable management and control systems to recognize, track, and handle common business risks, such as losses from improper business strategy execution, penalties and fines, negative cash flows, or unforeseen and excessively high operating expenses since these contribute to liquidity risks.
i. RSPs should tie the final settlement of one obligation to the final settlement of the other if it settles transactions involving the settlement of two linked obligations (such as foreign currency transactions) to mitigate principal risk. Measures to eliminate the principal risk should be taken by ensuring that the final settlement of one obligation occurs if and only if the final settlement of the linked obligation also occurs.
j. Ongoing evaluations are required to assess whether the RSP complies with industry standards for policies and practices related to liquidity risk. The assessments should cover internal controls, limitations, and important market developments.
k. RSPs should build and maintain connections with obligation holders, keep liabilities diverse, and ensure they can sell assets if needed.
l. An RSP that engages in activities with a more complex risk profile or that span multiple jurisdictions should consider retaining additional liquidity resources to cover a broader range of potential stress scenarios, including but not limited to the default of key participants and their affiliates, which would result in large aggregate payment obligations to the RSP in extreme but conceivable market conditions. The RSP's qualifying liquid resources in each currency must include cash in the bank, committed lines of credit, committed foreign exchange swaps, and committed repos, in addition to highly marketable collateral held in custody and investments that are easily accessible and convertible into cash with prearranged and highly reliable funding arrangements, even in extreme but plausible market

conditions. To the extent that the RSP owns collateral qualifying for pledging to (or engaging in other appropriate types of transactions with) the central bank, the RSP may count any access to normal credit at the issuing central bank as part of the minimum liquidity requirement. All of these resources should be available as needed.

m. RSPs may add additional types of liquid assets to their qualified liquid resources. If the RSP chooses to do so, then these liquid resources should take the form of assets that are most likely to be sold or accepted as collateral for loans, swaps, or repossessions on an as-needed basis after a default, even if this cannot be reliably prearranged or guaranteed in turbulent market conditions. Even if the RSP does not have access to routine central bank lending, it should consider the types of collateral the relevant central bank typically accepts because those assets may be more likely to be cash under pressure.

n. RSPs should gain a high level of confidence through due diligence that each provider of its minimum required qualifying liquid resources, whether an RSP participant or an outside party, understands and manages its associated liquidity risks and can fulfil its commitment as required. A liquidity provider's possible access to credit from the issuing central bank may be considered when determining how reliable their performance is regarding a specific currency. The RSP should regularly test its access procedures to its liquid resources at a liquidity provider.

o. Wherever possible, an RSP with access to central bank accounts, payment services, or securities services should use these resources to improve its liquidity risk management.

p. RSPs may hold liquid net assets funded by equity (such as common stock, disclosed reserves, or other retained earnings) to maintain operations and services as a going concern if it suffers general business losses. The amount of liquid net assets funded by the equity that the RSP can hold should be based on its overall business risk profile and the time needed to achieve a recovery or an orderly wind-down, as appropriate, of its critical operations and services if such action is taken. The RSP must keep a workable recovery or orderly wind-down plan in place and have access to enough liquid net assets backed by equity to carry it out.

q. RSPs must maintain enough liquid net assets supported by equity to cover current operating costs for at least six months. Stock held under international risk-based capital norms can be incorporated where applicable and appropriate to avoid redundant capital requirements. Assets retained to cover general business risk should be high calibre and have enough liquidity to enable the RSP to cover its current and anticipated operating costs under various circumstances, including challenging market conditions.

r. Should its equity fall close to or below the required amount, RSPs should continue to have a workable plan for obtaining further equity.

s. Understanding an RSP's on and off-balance sheet positions is essential for predicting future cash flows and determining how to meet financing obligations. This entails identifying the funding markets the RSP can access, comprehending their characteristics, assessing an RSP's present and prospective market use, and checking for any indications of confidence deterioration.

t. To effectively manage liquidity risk, a measuring and monitoring method is required. RSPs must compare their cash inflows and outflows to determine the possibility of net shortages. Static simulations based on existing holdings and straightforward calculations are two methods that can be used to assess liquidity risk. Monitoring market and economic movements is also crucial for managing liquidity risk. A mechanism for measuring and monitoring liquidity risk should assist in managing liquidity during times of crisis and maximizing return through the effective use of existing money.

u. Making estimates about upcoming financial requirements is a crucial component of managing liquidity. While it may be simple to quantify or estimate some cash inflows and outflows, RSPs must also make assumptions about their future liquidity needs in the short term and over longer time frames. The significance of the RSP's reputation in its capacity to borrow funds easily and on fair terms is an important issue to consider. Due to this, RSP personnel managing overall liquidity should be aware of any information (such as a disclosure of a decline in earnings or a downgrading by a rating agency) that may influence the market and the general public's perceptions of the RSP's soundness.

v. Credit and liquidity risks are closely related. RSPs should strictly monitor, manage, and restrict their credit and liquidity risks by, where possible and practical, executing their money settlements in their local bank funds to reduce credit and liquidity risks. If central bank funds are unused, RSPs should carry out their money settlements using a settlement asset with low credit or liquidity risk.

w. RSPs should set rigorous requirements for their settlement banks that consider, among other things, their regulation and supervision, creditworthiness, capitalization, accessibility to liquidity, and operational reliability and monitor adherence to those standards.

x. The concentration of credit and liquidity exposures to settlement banks should also be monitored and managed by an RSP. Minimizing and closely controlling credit and liquidity risks is important if it conducts money settlements in its accounts.

y. For an RSP and its participants to manage credit and liquidity risks, legal agreements with settlement banks, where applicable, should specify in detail when transfers on the books of specific settlement banks are expected to be final and that funds received should be transferable as soon as possible, ideally the same day and at the very least by the end of the day.

z. Some of the commonly used liquidity measurement and monitoring techniques and practices that RSPs may adopt include the following:

    i. Developing a contingency funding plan, i.e., a set of rules and guidelines that help an RSP to promptly and affordably satisfy its funding requirements. In this strategy, future cash flows and funding sources of an RSP are projected under various market scenarios, such as aggressive asset expansion or quick liability erosion. A solid plan considers the RSP's institutional structure, risk exposure, business size, nature, and complexity. The plan includes a quantitative study of cash flow predictions, matching prospective cash flow sources and needs, and establishing indicators that alert management to potential hazards. The contingency plan should specify individual roles and duties in the event of liquidity challenges and include asset-side and liability-side solutions to cope with liquidity issues.

    ii. Using a maturity ladder, i.e., there should be longer periods after measuring short-term exposures. This represents a daily gap for the following one to two weeks, a monthly gap for six to twelve months, and so forth. When estimating cash flows, it is crucial to consider the finance requirements and behavioural factors rather than contractual maturity, prior experiences, seasonality, and economic cycle phases.

    iii. Setting liquidity ratios and limits, i.e., may also be used to set boundaries for managing liquidity. Always combine ratios with more detailed information regarding borrowing power, creditability, and transaction volume.

    iv. Reviewing assumptions in liquidity management, i.e., plans and assumptions, must be regularly examined to determine their continued validity. An RSP's future liquidity situation will be impacted

by elements that are not always predictable with accuracy, especially given how quickly the markets can move.

v. Putting in place a management information system is crucial for making decisions regarding liquidity management because efficient liquidity management may require daily internal reporting. Information should be easily accessible for daily risk control and liquidity management. Data must be properly organized, thorough yet succinct, targeted, and readily available. A management information system can also verify that an RSP is adhering to its defined policies, processes, and limits and any regulatory requirements regarding liquidity. Additionally, it helps management to assess the direction and magnitude of trends in the RSP's overall liquidity exposure. The RSP's liquidity management procedures, hazards, and legal obligations determine the reports' structure and substance.

vi. Putting in place internal controls, i.e., effective internal controls to guarantee the reliability of procedures for managing liquidity risk. Internal controls support effective and efficient operations, accurate financial and regulatory reporting, and adherence to all applicable laws, rules, and organizational policies. The factors of liquidity risk management must be regularly assessed and reviewed. This includes ensuring that staff adhere to established policies and procedures and that those procedures achieve the goals for which they were designed. Any material change that could affect the efficiency of controls should be covered in these reviews and assessments.

6.2.2 Foreign Exchange Risk Management Guidelines

An RSP must implement foreign exchange risk mitigation measures and know the variables that could drive this risk category. RSPs should keep additional financial resources sufficient to address foreign exchange exposures.

The formality and sophistication of the RSP's foreign exchange risk management framework should be commensurate with the RSP's size and risk profile.

Assessment, Monitoring, and Control of Foreign Exchange Risk

a. RSPs should set up an effective and thorough foreign exchange risk management process that includes a framework for identifying, assessing, and monitoring this risk category.
b. RSPs should put in place an appropriately detailed structure of risk limits, guidelines, and other parameters that can be used to regulate foreign exchange risk-taking.
c. Understanding the amount at risk and how exchange rate fluctuations affect this risk exposure is essential for its management. Sufficient information must be readily available to allow appropriate action to make these decisions within reasonable periods.
d. RSPs should incorporate their foreign exchange risk management process into their overall risk management system. As a result, the RSP would be better equipped to comprehend and control its consolidated risk exposure. Where applicable, the risk management process should be integrated with the group, if any, where the RSP is a member.
e. RSPs may assess their exposure to foreign exchange risk using various methods. RSPs may consider methods suited for the scope and nature of their activities involving foreign exchange risk, the management personnel's expertise and experience, and the capability of systems for monitoring and reporting foreign exchange risk.

f. If applicable, RSPs should ensure that their valuation procedures for treasury and financial derivatives are reliable and separate from their trading role. When employed in valuations and stress testing, models and the underlying statistical analyses should be suitable, consistently applied, and based on reasonable assumptions. Before deployment, these should be validated. Models and analyses should be checked regularly to ensure that position data is correct, that volatility, value, and risk factor calculations are accurate, and that the correlation and stress test assumptions are fair. More regular assessments are required if models or assumptions alter due to changes in foreign exchange conditions.

g. If applicable, setting restrictions on the size of the net open position in each currency in which an RSP is permitted to have exposure and the total of all currencies could be one of the strategies. The total assets or core capital ratio may be used to represent this. Additional methods include changing the net open position, increasing the foreign assets/liabilities ratio, and using the foreign currency assets to foreign currency liabilities ratio, among others.

h. Depending on the nature and complexity of an RSP's activities, hedging techniques may be used in managing and limiting foreign exchange risk. In this context, various financial instruments, including derivative products, can be used to hedge. Some examples include foreign currency swaps, foreign currency options, and foreign forward exchange contracts. Financial instruments used for hedging cannot be distinguished from those that could be utilized to take risk positions. RSPs must ensure that the hedging technique is understood and the instrument cost-effectively satisfies its specific requirements before employing the hedging products.

i. The overall risk exposure of the RSP as a result of a potential change in the asset/liability mix and other risk exposures, including credit and foreign exchange risks, should be considered when evaluating the success of the hedging efforts. For instance, in foreign currency swaps, credit risk is used to replace foreign exchange risk (the risk that the counterparty to the swap may be unable to fulfil its obligations). In this situation, hedging actions must be carried out following a clear hedging strategy, the ramifications of which the RSP fully comprehends under various foreign exchange situations. It is crucial to understand the goals and restrictions of utilizing hedging instruments to ensure that the hedging methods effectively manage exposure rather than unintentionally assume additional or alternative types of risk.

j. Before using derivative instruments for position-taking or hedging, RSPs must be sure that the necessary policies and procedures, as well as the ability to put them into effect, are in place.

k. Regular scenario analysis and stress tests should be a part of the foreign exchange risk management process where applicable. RSPs may select scenarios using empirical models of changes in foreign exchange risk factors or historical data analysis. The goal should be to enable RSPs to determine how substantial changes in foreign exchange risk factors may affect its assets and financial situation. As a result, the chosen scenarios may include low-probability negative possibilities that result in massive losses. Stress tests and scenario analysis should be quantitative as well as qualitative.

l. Scenario analysis and stress testing should be carried out throughout the entire RSP, considering the implications of unusual changes in foreign exchange and non-foreign exchange risk factors. The scenarios include but are not limited to changes in fees, foreign exchange liquidity, historical correlations, maximum cash inflow and outflow assumptions, the RSP's susceptibility to worst-case situations, or the default of a substantial counterparty.

m. Stress testing and scenario analysis would help the board of directors and management personnel better understand the possible effects of various fluctuations in foreign exchange on the operations, earnings, and capital positions of an RSP. The outcomes of scenario analyses, stress tests, and key underlying assumptions should be frequently reviewed by the board of directors and management personnel. The outcomes should be considered while developing and revising policies and constraints. Depending on the potential losses predicted by the scenario analysis and stress testing and the likelihood of such losses, the board of directors and management staff may take additional steps to mitigate risks or build contingency plans.

n. The board of directors should regularly evaluate reports outlining an RSP's exposure to foreign exchange risk. Although the reports created for the board and different levels of management personnel will vary depending on the foreign exchange risk profile of an RSP, they should at the very least include summaries of the RSP's aggregate foreign exchange risk exposures, such as the results of foreign exchange risk stress tests, the maturity distribution of foreign currency denominated assets and liabilities by currency, and summaries of the findings of reviews of foreign exchange risk. Internal and external auditor findings, or the findings of any other independent reviewer, relevant to this risk category, as well as a summary of outstanding contract amounts by settlement date and currency, both spot and forward, compliance reports, and daily foreign exchange operations gain/loss, should be included.

o. RSPs should routinely assess their foreign exchange risk management strategy considering both their financial performance and foreign exchange changes. All changes and exclusions must get the board's approval and be conveyed to the concerned personnel.

p. The following are some of the typical liquidity assessment and monitoring methods and procedures that RSPs may use:

    i. Management information systems.

        - Controlling foreign exchange risk exposure requires an accurate, comprehensive, and fast management information system to inform management personnel and promote adherence to the risk management policy. Risk measures should be reported regularly and should make a clear comparison between existing exposure and policy restrictions. Previous forecasts or risk estimations should be contrasted with the actual outcomes to spot flaws.
        - The scale, complexity, and breadth of an RSP's trading, other financial activities, and the foreign exchange risk it assumes should all be considered when designing the risk management system. It should also make it possible to identify precisely and appropriately, measure, monitor, and regulate the different foreign currency risk exposures. On an RSP-wide basis, all substantial risks should be quantified and combined.
        - The risk management system of RSPs should be capable of estimating risk exposures and continuously tracking modifications in foreign currency risk variables and other foreign exchange conditions. The RSP should keep track of its risk profile on an intra-day basis if its risk levels.
        - Wherever practicable, the risk management system should be able to calculate the likelihood of future losses. Additionally, it should make it possible for an RSP to quickly recognize risks and respond to negative trends in foreign exchange factors by taking appropriate corrective action.

ii. Internal controls

- Adequate internal controls are necessary to ensure the integrity of the foreign exchange risk management process. The internal controls should encourage efficient and successful operations, trustworthy financial and regulatory reporting, and adherence to pertinent laws, rules, and organizational policies.
- Limits for foreign exchange risks should be established in accordance with the highest exposures permitted by the policy. It is necessary to define risk management rules, establish methods for identifying, measuring, and assessing foreign exchange risk, and keep track of an RSP's adherence to defined policies and foreign currency risk limits.
- RSPs should regularly have an independent party to review and evaluate the assessment, monitoring, and control procedures. An independent reviewer must ensure that the risk measuring system used by the RSP is adequate to account for all substantial aspects of foreign currency risk, whether they originate from on- or off-balance sheet activities.
- Positions in critical sections of the risk management process should be adequately separated to avoid conflicts of interest. Management should ensure adequate safeguards to reduce the possibility that people in risk-taking positions may inadvertently influence critical risk-control functions such as developing and enforcing policies and procedures, disclosing risks to management, and performing back-office tasks. Such safeguards should be of a type and extent appropriate to the RSP's size and structure. They should also be appropriate for the quantity and complexity of foreign exchange risk to which RSPs are exposed and the complexity of their transactions and commitments.
- Ensure distinct and effective separation of duties between people who initiate transactions and those who oversee operational tasks such as arranging quick and correct settlements, exchanging and reconciling confirmations, or keeping track of foreign exchange activity.
- Procedural controls should be in place to guarantee that transactions are accurately paid for and properly recorded in the RSP's records and accounts.
- Controls should be set up so management personnel are immediately notified of unauthorized trading. Moreover, the controls should guarantee that excesses in foreign exchange activity are recorded and regularly checked against the RSP's foreign exchange risk, counterparty, and other limits.
- Independent audits must partially monitor an RSP's foreign exchange risk management programme. RSPs should apply these to guarantee adherence to and the reliability of the foreign currency risk rules and procedures.
- Independent audits should be performed on an RSP's foreign exchange risk management efforts over a reasonable period to ensure that policies and procedures are implemented and adequate management controls over foreign exchange positions are in place. The audits should confirm the sufficiency and accuracy of management information reports regarding the RSP's foreign exchange risk management activities, as well as ensure that personnel involved in foreign exchange risk management have access to accurate and complete information regarding the RSP's foreign exchange risk policies and risk limits, as well as the knowledge required to make decisions in accordance with risk management policies.

- The board of directors of the RSP should promptly receive assessments of the foreign currency risk activities for review. Discovered material weaknesses should receive prompt, appropriate high-level attention and management personnel should be rigorously examined and confirmed in their efforts to remediate those flaws.

6.2.3 Interest Rate Risk Management Guidelines

RSPs must implement interest rate risk mitigation measures and be aware of the variables that could drive this risk category. RSPs should keep additional financial resources sufficient to address interest rate exposures.

The formality and sophistication of the RSP's interest rate risk management framework should be commensurate with the RSP's size and risk profile.

Assessment, Monitoring, and Control of Interest Rate Risk

a. Implement an integrated view of interest rate risk across products and business lines. An RSP board of directors, management team, and staff must be sufficiently equipped to manage interest rate risks, including taking the necessary activities to measure, monitor, and control them while adhering to the strategies.
b. RSPs should implement strategies to minimize risks and ensure adherence to rules, laws, and regulations.
c. RSPs should establish reasonable risk restrictions, create criteria for valuing positions, and assess performance.
d. RSPs should consider constructing a portfolio mix to protect the RSP from rising interest rate exposures.
e. RSPs should consider the market's economic and interest rate conditions and their effects on interest rate risk while formulating mitigation measures, taking into account whether the RSP management personnel and other staff have the knowledge necessary to profit under a particular circumstance and can recognize, track, and manage the interest rate risk in the market.
f. The interest rate risk control strategy for the RSP should be frequently reviewed while considering its financial performance and changes in market interest rates. All modifications and exclusions must be approved by the board of directors and disseminated to the relevant personnel.
g. Wherever practical, RSPs should have a unit, or a person specifically charged with managing interest rate risks. This unit would create and uphold the necessary risk management guidelines, reporting requirements, and supervision programmes.
h. RSPs should design a reliable and thorough risk management procedure with a framework to recognize, quantify, and keep track of interest rate risk. The RSP should also design a detailed framework for risk limits, rules, and other criteria that will be used to manage interest rate risks.
i. Depending on the nature, scale, and complexity of its trading and other financial operations and the interest rate exposures it has taken, RSPs may implement a management information system (MIS) for managing, monitoring, and reporting interest rate risk. It should also make it possible to quantify, monitor, and control the different interest rate risk exposures precisely and appropriately. Monitoring changes in interest rate risk variables and other interest rate conditions should be possible with the aid of the risk management system. RSPs should keep track of their risk profile intra-day if their risk levels

change dramatically over a trading day. Wherever practicable, the risk management system should be able to calculate the likelihood of future losses. Moreover, it should make it possible for an RSP to recognize risks well in advance and respond quickly to negative changes in interest rate components.

j. The basis, yield curve, repricing, and option risk exposures should all be considered by the interest rate risk measuring system of an RSP. Most often, the aggregate risk profile of the RSP will be dominated by the interest rate characteristics of its largest holdings. While all RSP holdings should be treated properly, measurement methods should rigorously assess such concentrations. Even though they do not constitute a big concentration, interest rate risk measurement systems should rigorously treat those instruments since they may considerably impact the RSP's overall position. Special consideration should be given to instruments having considerable embedded or explicit option characteristics.

k. A maturity/re-pricing schedule is the first step in the most basic methods for calculating an RSP's interest rate risk exposure. It divides interest-sensitive assets, liabilities, and off-balance sheet positions into 'time bands' based on their maturity (if fixed rate) or the amount of time until their subsequent re-pricing (if floating rate). These schedules can produce straightforward indicators of how sensitive earnings and economic values are to interest rate risk. This method is commonly known as gap analysis when it is used to evaluate the interest rate risk associated with current earnings. A measure of an RSP's re-pricing risk exposure is the gap size for a specific time band, calculated as assets less liabilities plus off-balance sheet exposures that re-price or mature within that time band.

l. By assigning sensitivity weights to each time band, a maturity/re-pricing schedule can also be utilized to assess how changing interest rates affect the economic value of the RSP. These weights are often determined by estimations of the assets' and liabilities' durations, where duration measures how much an asset's economic value will vary, given a slight change in the level of interest rates. Duration-based weights can be employed with a maturity/repricing schedule to offer a reasonable estimate of the RSP's economic value change that would occur given a specific set of interest rate changes.

m. More advanced simulation techniques may be used in interest rate risk measurement systems. Simulation techniques sometimes involve comprehensive assessments of the potential consequences of changes in interest rates on earnings and economic value by projecting the future trajectory of interest rates and their impact on cash flows. The cash flows resulting only from the RSP's current on- and off-balance sheet positions are evaluated in static simulations. In a dynamic simulation technique, the simulation incorporates more specific assumptions regarding the direction that interest rates will take in the future and anticipated changes in the business activity of the RSP during that period. These more advanced methods better account for the impact of embedded or explicit options and enable the dynamic interaction of payment streams and interest rates.

n. Regardless of the measuring system, the accuracy of the fundamental methodology employed to calculate interest rate risk exposure determines the efficacy of any strategy. RSPs should ensure that the level of detail about the nature of their interest-sensitive holdings is proportionate to the complexity and risk inherent in those positions when designing interest rate risk measurement systems. For instance, using gap analysis, the number of time bands into which positions are aggregated influences the accuracy of interest rate risk estimation. Aggregating holdings and cash flows into large time bands always leads to some precision loss. To decide how much aggregation and simplification should be incorporated into the measuring approach, the RSP must evaluate the relevance of the probable loss of precision.

o. Forecasts of the likely direction of future interest rates are used in some way in estimates of interest rate risk exposure, regardless of whether they are connected to earnings or economic value. RSPs should consider an interest rate change that is substantial enough to cover the risks associated with its holdings for risk management reasons. The RSP should consider using various scenarios, including those that could impact potential changes in the relationships between interest rates and general changes in interest rate levels. Simulation approaches could be used to predict likely changes in interest rates. Moreover, statistical analysis might be crucial in assessing correlation hypotheses about basis or yield curve risk.
p. It is critical to comprehend the underlying assumptions of the risk measurement system while evaluating the outcomes of interest rate risks. At least once a year, key assumptions should be reevaluated and well-documented.

6.2.4 Credit Risk Management Guidelines

Credit exposures to participants and those resulting from RSP payment, clearing, and settlement procedures should be adequately measured, monitored, and controlled. RSPs should therefore put sound basic principles into practice that make it easier to identify, measure, monitor, and control credit risk. This includes ensuring that sensible procedures, suitable plans, and effective practices for credit risk management are in place. Additionally, RSPs must maintain accurate records of exposures and have policies for granting credit to counterparties or agencies. The overall risk appetite concerning credit risk should be outlined, and RSP's large exposure to credit risk should be kept sensible and compatible with the available capital.

The formality and sophistication of an RSP's credit risk management framework should be commensurate with the RSP's size and risk profile.

Assessment, Monitoring, and Control of Credit Risk

a. To control credit risk, RSPs should identify sources of credit risk, regularly assess and track, measure and monitor credit exposures, and employ proper risk management techniques. To measure and track its credit exposures to its participants and the credit risks associated with its payment, clearing, and settlement processes, RSPs need to build up a solid strategy, policy, and credit administration processes. The strategy and policy should consider that credit exposure may arise from current and potential future exposures.
b. RSPs should establish the general structure for credit or credit relationship approving authority and expressly delegate credit sanctioning responsibility to the appropriate functions.
c. Establishing internal controls, including clear lines of authority and accountability, is necessary to ensure an efficient credit risk management process. It is also necessary to put in place lines of communication to ensure the timely distribution of credit risk management policies, procedures, and other information to all participants.
d. The credit-granting approval procedure used by RSPs should specify who is responsible for decisions made and who has the authority to authorize credits or changes to credit terms.
e. Requirements should specify who is eligible for credit, how much credit they are eligible for, the available credit types, and the conditions under which credit should be issued. Among others, on the

decision-making ladder, a credit analyst with experience appropriate to the size and complexity of the transaction should carefully examine each credit proposal.

f. RSPs should use margin and other pre-funded financial resources to confidently cover all their current and future exposures to each participant. Additionally, an RSP that engages in riskier activities with a more complex risk profile or that is systemically substantial across multiple jurisdictions should keep additional financial resources on hand to cover a variety of possible stress scenarios, including but not limited to the default of the participants and their affiliates that could potentially result in credit exposure to the RSP. Rigorous stress testing would enable RSPs to calculate the amount and periodically assess the sufficiency of its overall financial resources in the event of a default or a series of defaults.

g. To help reduce the risks associated with certain credits, an RSP can use credit risk mitigants, including collateral, guarantees, credit derivatives, or on-balance sheet netting.

h. An RSP that needs collateral to control the credit exposure of either itself or its members should only accept collateral with low credit, liquidity, and market risks. A well-designed, functionally adaptable collateral management system should be used. Haircuts that are routinely tested should be built, considering stressful market situations and prudent valuation methods. RSPs should avoid holding a large amount of a particular asset because it would make it difficult to swiftly sell the asset without suffering severe price consequences. While accepting cross-border collateral, RSPs should take precautions to reduce any potential risks associated with its use.

i. RSPs should have regulations governing the acceptance of different types of collateral, procedures for continuously evaluating such collateral, and a mechanism to guarantee that collateral is and remains enforceable and realizable. The RSP should assess the level of coverage being offered for guarantees concerning the creditworthiness and competence of the guarantor.

j. Yet, the strength of the counterparty's ability to repay should be the main consideration when entering into a credit transaction. Credit risk mitigation techniques should not be used in place of thorough evaluations of the borrower or counterparty's ability. It should be understood that any credit enforcement procedures (such as foreclosure proceedings) usually result in the transaction's profit margin loss. Moreover, RSPs must be aware that the same factors that have reduced the credit's potential to be recovered may harm the value of the collateral.

k. It is crucial to determine the agent or counterparty's integrity and reputation, current risk profile (including the types and aggregate amounts of risks), repayment history, current capacity to repay based on past financial trends and cash flow projections, forward-looking analyses of the capacity to repay based on various scenarios, and the agent or counterparty's legal capacity.

l. RSPs must become familiar with the agent or counterparty and ensure they work with a person or organization of good standing and creditworthiness before beginning any new credit relationship. Strict rules must be in place, in particular, to prevent affiliation with people engaged in fraud and other crimes. This can be done in several ways, such as by requesting recommendations from known people, contacting credit reference agencies, knowing the people in charge of managing the counterparty business and checking their references and financial standing. Nonetheless, RSPs should not extend credit to a counterparty just because they know them or believe they have a good reputation.

m. RSPs should use updated data on the obligor's financial and business conditions and account conduct while conducting a credit check. The impact of any exceptions found throughout the credit monitoring procedure on the obligor's creditworthiness should also be considered.

n. The basic requirements for the information upon which the analysis is based should be established via an efficient evaluation procedure. The information and paperwork required to approve new credit relationships, renew current credit relationships, and/or alter the terms and conditions of previously approved relationships should be governed by policies. The information obtained will serve as the foundation for any internal assessment or rating given to the credit, and management personnel's capacity to make informed decisions about the acceptance of the credit depends on how accurate and thorough the information is.

o. RSPs should evaluate the counterparty's overall profitability and the risk/return relationship. Credit facilities should be priced to cover all underlying expenses and compensate the RSP for risks. The RSP must weigh the risks against the expected return when determining whether and how much credit to extend, considering both price and non-price terms such as collateral, restrictive covenants, etc.

p. When evaluating credit risk, RSPs should consider potential negative outcomes and their potential effects on counterparties or borrowers.

q. When evaluating possible credit extensions, RSPs must consider keeping sufficient capital to absorb risks and unforeseen losses and prepare for anticipated losses.

r. RSPs should have procedures to determine when it is reasonable to designate a group of borrowers as related counterparties and as a single borrower when evaluating credits. Exposure to groupings of accounts, whether corporate or non-corporate, with connections such as common management and family ties or under common ownership or control, would be included in this.

s. RSPs must monitor the amount of credit given and grant it to such parties on an arms-length basis. No board member or management personnel, or staff should participate in the processing and approval procedure if they stand to gain from the transaction.

t. Establishing exposure limits for counterparties and groups of connected counterparties that aggregate various risks is crucial to credit risk management. The counterparty's creditworthiness, a genuine need for credit, the state of the economy, and the RSP's risk tolerance should all be considered when determining the limit levels. Limits should also be set for respective products and/or geographic regions to avoid concentration risk.

u. Credit reviews should be carried out quarterly. However, they should be carried out more frequently for newly opened accounts where RSPs might not be familiar with the obligor and for categorized or negatively rated accounts with higher default risks.

v. Credit risk management is crucial to preserving an RSP's stability and security. Administration entails maintaining a current credit profile, gathering financial data, keeping track of repayments, sending out notices, and creating various documents such as credit agreements, monitoring documentation, contractual requirements, legal covenants, collateral, accuracy and timeliness of information provided to management information systems, adequacy of controls, and compliance with established policies and procedures as well as applicable laws. RSPs must guarantee the availability of all the information required to determine the agent's or counterparty's current financial status and enough information to trace the decisions made and the credit history.

w. To enable efficient analysis, sound and prudent management, and control of current and potential credit risk exposures, RSPs must ensure the development and implementation of an appropriate reporting system concerning the content, format, and frequency of information regarding the credit

portfolio and credit risks. The system should be able to monitor the quality of the credit portfolio, uncollectible credits written off, and probable losses, among other functionalities.

x. RSPs need to articulate a system that enables them to monitor the performance of the obligors on a day-to-day basis and take remedial measures as and when any deterioration occurs. RSPs could use such a system to determine whether the extended facilities are being serviced under the terms and conditions, the sufficiency of provisions, whether the total risk profile is within the set boundaries, and compliance with regulatory constraints.

y. The internal audit function should review the credit operations to assess whether or not the RSP's policies and procedures are adequate and being adhered to. In addition to the general risk management guidelines on strategy and policy documents highlighted earlier, the following should be part of the policies:

- An outline of how RSPs intend to extend credit depending on products, locations, currencies, maturities, levels of concentration and diversity, and pricing tactics of various agents or counterparties' market segments. The credit procedures should aim to understand the RSP's agents or counterparties, their credentials, and their businesses to know their customers.
- A framework for investment choices and credit extensions that reflects an RSP's credit risk tolerance.
- An outline of the general traits and qualities of an agent or counterparty with whom the RSP is prepared to engage or is prohibited, such as the kind of credit facilities or relationships, the kind of collateral security, the geographic locations, or the types of industries.
- Credit evaluation/appraisal procedure, administration, and documentation.
- Credit approval authority at different levels of hierarchy, including the authority to approve exceptions such as credit extension beyond set limits, concentration limits on individual counterparties and groups of connected counterparties, and specific economic sectors, geographical regions, and product categories.
- Specific limits or restrictions imposed by a regulator aligned with internal exposure limits.
- Information on who can approve write-offs and allowances for probable losses, credit pricing, the roles and responsibilities of the units and staff involved, how to handle extended problematic credit, and internal rating systems, including information on what each risk grade entails.
- Clarity of provisions on credit losses due to individual or collective participant defaults concerning any of their RSP-related commitments.
- The allocation of potential uncovered credit losses and the return of any money RSPs may borrow from liquidity providers.
- An outline of the RSP's approach for replenishing any financial resources that the RSP may use during a stressful event.
- Default management provisions enable the RSP to respond quickly to losses and liquidity difficulties to continue fulfilling its obligations. A participant default should not prevent the RSP from continuing to fulfil its duties. RSPs should therefore include default rules and procedures that cover the replenishment of resources after a default. All applicable discretionary procedures should be specified.
- Testing and evaluation methodology of an RSP's default procedures, including any close-out. For the rules and processes to be useful and effective, such testing and evaluation should be carried out at least once a year or after substantial changes.

6.2.5 Operational Risk Management Guidelines

Operational risks for RSPs involve exposures from technology, strategic, compliance (legal), and country risks. RSPs should set up a robust operational risk management framework with the required strategy and policy to identify, measure, monitor, and control operational risks. The policy should include systems, rules, procedures, controls, risk tolerance, and the RSP's prioritization of operational risk management activities, including the extent of and how operational risk is transferred outside the RSP. The framework should define the RSP's strategy for recognizing, assessing, monitoring, and controlling/mitigating the risk.

The formality and sophistication of the RSP's operational risk management framework should be commensurate with the RSP's size and risk profile.

Assessment, Monitoring, and Control of Operational Risk

a. Risk identification is essential for a functional operational risk monitoring and control system. Effective risk identification considers internal and external factors that could harm the attainment of an RSP's goals. Such factors include the RSP's structure, the nature of its activities, the technologies in use, the calibre of its human resources, organizational changes, and employee attrition.
b. To detect and assess operational risk, RSPs must conduct self-risk assessments, whereby an RSP evaluates its operations and endeavours to draw up a list of possible operational risk vulnerabilities. This internally driven process frequently includes workshops and/or checklists to determine the advantages and disadvantages of the operational risk environment.
c. Risk mapping is also an important resource in detecting and assessing operational risk. Different divisions, functions, or process flows are mapped according to the categories of operational risks they face. This activity might highlight weaknesses and help organize the next initiatives.
d. Moreover, RSPs may incorporate scenario analysis and a risk assessment checklist.
e. A test of due diligence can be conducted, monitoring the actions of third-party providers, particularly those who lack remittance industry knowledge, and regularly assessing this process. RSPs may need to consider backup plans for crucial tasks, such as the availability of alternative external parties and the costs and resources needed to switch external parties when needed.
f. RSPs should be aware of potential consequences on their operations and customers of any potential service shortcomings provided by vendors and other third-party or intra-group service providers, including operational breakdowns and the external parties' potential business failure or default.
g. The board of directors and management personnel should ensure that each party's obligations and expectations are specified, understood, and enforced. The risk assessment should expressly consider the extent of the external party's liability and financial capacity to reimburse the RSP for mistakes, negligence, and other operational failures.
h. Once RSPs have identified operational risks, control mechanisms intended to address those risks must be formulated. RSPs must choose whether to take a risk or apply suitable measures to mitigate all material operational risks that have been identified. When faced with risks that cannot be mitigated, RSPs must determine whether to accept them, scale back on the number of business activities involved, or stop all operations altogether. Knowing that some substantial operational risks have low probabilities, but potentially very large financial impacts is important. Moreover, not all risk events

can be controlled, for example, natural disasters. Tools or programmes for risk reduction can be utilized to lessen the vulnerability to, frequency of, or severity of such incidents. For instance, insurance coverage can externalize the "low frequency, high severity" risk that could emerge from third-party claims caused by mistakes and omissions, actual loss of securities, employee or third-party fraud, and natural disasters.

i. Moreover, RSPs should deem risk mitigation technologies as an addition to effective internal operational risk controls rather than as a substitute for them. Exposures can be substantially decreased by implementing systems that promptly identify and fix operational risk mistakes. The extent to which risk mitigation measures, such as insurance, decrease risk, shift the risk, or even generate a new risk, such as legal or counterparty risk, must be carefully considered.

j. Investments in proper processing technology and information technology security are crucial for risk reduction. RSPs should be aware, however, that greater automation may cause high-frequency, low-severity losses to change into low-frequency, high-severity losses. The latter may be connected to service loss or prolonged disruption brought on by internal issues or circumstances beyond an RSP's immediate control, such as outside events. Such issues can pose serious challenges for RSPs and endanger their capacity to carry out crucial business operations. RSPs should, for example, create business continuity and disaster recovery plans that address this risk.

k. To effectively manage operational risk, a monitoring process must be in place. Frequent monitoring of operations can make it easier to spot and address deficiencies with operational risk management rules, processes, and procedures. The potential frequency and/or severity of a loss occurrence can be substantially decreased by quickly identifying and correcting these deficiencies. Monitoring frequency should be determined by the vulnerabilities involved and the frequency and type of operational environment changes. RSPs' actions should include monitoring as their natural element. The outcomes of these monitoring efforts and compliance evaluations undertaken by the risk management and internal audit departments should be included in regular management personnel and board of directors reports.

l. In addition to monitoring operational risk events, RSPs must identify the appropriate indicators to give an alert before downside risk becomes more probable. Such indicators (also referred to as critical risk indicators or early warning indicators) should be forward-looking. The early warning system should reflect prospective operational risk sources, such as rapid expansion, the launch of new products, personnel turnover, transaction errors, system outages, etc. RSPs can take appropriate action in response to key material concerns when thresholds are closely connected to these indicators through efficient monitoring procedures. Examining the risk indicators, such as financial trends, can give information on the operational risk RSPs face. These indicators must be examined regularly, such as monthly or quarterly, to notify RSPs of any changes that might be a sign of concern. Some indicators include unsuccessful deals, personnel turnover rates, and the frequency and/or seriousness of errors and omissions. These indicators might be linked to thresholds or limits so that when exceeded, management personnel would be aware of potential exposure areas.

m. Analysing historical loss data from RSPs may also help determine how exposed they are to all the components of the operational risk and help create policies to reduce or eliminate that risk. Establishing a structure for methodically tracking and recording the frequency, severity, and other pertinent information on individual loss incidents is an efficient way to make excellent use of this information.

n. A reliable management information system (MIS) is required to monitor operational risk effectively. With the aid of MIS, RSPs should be able to quickly assess and monitor all the components of their operational risk and produce statistics and reports for the board of directors and management personnel.

o. The risk management office, business units, and the internal audit function should report to management personnel regularly on internal financial, operational, and compliance data, as well as information from the outside market, pertaining to situations and occurrences that are important for decision-making. Reports should be provided to the appropriate management levels and RSP divisions in areas where risky incidents may occur. Reports should accurately reflect identified problem areas and urge swift solutions to outstanding issues. The management personnel should routinely check the timeliness, correctness, and applicability of reporting systems and internal controls to ensure these reports' usefulness and dependability. Additionally, the management personnel may assess the efficacy and reliability of internal reports using other reports created by outside parties such as external auditors, regulators, or supervisors. Reports should be reviewed to build new risk management policies, processes, and practices and enhance current risk management performance. The board of directors should be provided with enough higher-level information to enable them to comprehend an RSP's overall operational risk profile and concentrate on the strategic and material implications for the RSP.

p. Although a formal, written structure of policies and procedures is essential, it must be supported by a robust control culture that encourages reliable risk management techniques. Establishing an internal control culture where control activities are an essential component of an RSP's routine operations is the responsibility of the board of directors and management personnel. Controls essential to daily operations allow for swift reactions to evolving circumstances and prevent needless expenditures.

q. RSPs should ensure that other internal procedures are in place to control operational risk and segregate roles. Maintaining safeguards for access to and use of RSP's assets and records, ensuring that staff members have the necessary expertise and training, and identifying business lines or products where returns appear to be out of line with reasonable expectations, such as when a supposedly low risk, low margin trading activity generates high returns that could raise the question of whether such returns are indeed reasonable, are important.

r. Tasks must be properly segregated for an internal control system to be effective. Employees cannot be given responsibilities that could put them in a conflict of interest. When individuals or a team are given such competing responsibilities, they may be able to hide losses, mistakes, or improper behaviour. As a result, areas that could lead to conflicts of interest should be found, reduced, and carefully monitored by an independent party.

s. Internal procedures for reducing operational risk include routinely verifying and reconciling transactions and accounts.

t. An RSP is expected to have an internal audit function to ensure operating policies and procedures are properly applied. The board of directors should ensure that the audit programme's scope and frequency are proportionate to the risk exposures. Periodically checking the effectiveness of the RSP's operational risk management system should be done through the internal audit function.

u. The board of directors should ensure that the internal audit function is independent to the extent that it reviews the operational risk management framework. If the audit function is intimately involved in

the operational process for risk management, its independence can be jeopardized. Although it may offer useful advice to those in charge of operational risk management, the audit function shouldn't have any direct operational risk management duties.

v. Systems, operational rules, procedures, and controls should be evaluated, audited, and tested periodically and after substantial changes.

w. In addition to the general risk management guidelines on strategy and policy documents highlighted earlier, the following can specifically be included in the operational risk strategy and policy documents:
   - The policy should establish a procedure to guarantee that every new or changed service or system would be assessed for operational risk before going into effect.
   - Operational risks can be more noticeable when an RSP starts new operations, creates new products, enters uncharted markets, or operate enterprises far from their headquarters. This is especially true when these activities or products conflict with the RSP's main business strategies. Therefore, RSPs must ensure that the revision of policies and procedures considers these.
   - The policy should address the handling of the risks associated with outsourcing activities. Outsourcing activities can reduce an RSP's risk profile by transferring activities to others with greater expertise and scale to manage the risks associated with specialized business activities. However, the fact that an RSP uses third parties does not lessen the duty of the board of directors and management personnel to ensure that any third-party activity is done responsibly and in accordance with the law. Robust contracts and/or service-level agreements provide a detailed division of duties between external service providers. Additionally, RSPs must control any remaining risks related to outsourcing agreements, such as service interruptions.
   - An RSP policy should explicitly outline its responsibilities for delivering intangible and physical goods or tools and identify, monitor, and control the risks of such deliveries. The rules of an RSP must specify the obligations of the RSP concerning the supply of goods and services. The risks and expenses related to storage and delivery should be identified, monitored, and managed by an RSP.
   - RSPs should have policy provisions to help them accomplish their operational reliability objectives and clearly defined operational reliability objectives.
   - RSPs must ensure their operational risk policy provides scalable capacity to handle rising stress volumes and meet its service-level goals.
   - Comprehensive physical and information security policies that cover all potential weaknesses and threats should be provided in the policy.
   - The policy should describe key players, other RSPs, and service and utility suppliers that are potential threats to an RSP's operations and how such threats should be identified, monitored, and managed. Additionally, the policy must provide for recognition, monitoring, and controlling of any vulnerabilities its operations may bring to other RSPs.

(i) Technological Risk Management Guidelines

a. RSPs must use efficient risk management techniques, such as routine monitoring of crucial systems and networks, testing and patching software vulnerabilities, establishing cybersecurity policies, and maintaining a robust disaster recovery plan to reduce technological risk.

b. RSPs should implement information technology (IT) security measures in line with a board-approved policy to mitigate technological risk for the safety and security of the payment systems. After any

security event or breach, following a substantial change to the infrastructure or methods, RSPs should assess their security policy at least once a year to ensure it addresses safety and security, risk reduction, and fraud prevention. The policy should include effective mechanisms to identify and limit fraudulent transactions. In the event of suspicious operations, appropriate internal and external escalation measures must be in place, in addition to warning all key stakeholders, including customers.

c. The policy may also include mechanisms for velocity checks on the volume of transactions made with an instrument. RSPs should make sure that the policy is adhered to effectively.
d. In accordance with the scope and complexity of the RSP's operations, disaster recovery and business continuity plans should be developed, considering several situations to which the RSP may be subject. The business continuity plan must handle situations with a high chance of operations being disrupted, such as situations where a major or widespread disruption may occur. Using a backup location should be part of the plan and ensure crucial IT systems can resume functioning within two hours of disruptive events. Even under the worst-case scenario, the plan should be set up to allow an RSP to finish settlement by the end of the disruption day.
e. RSPs should regularly assess and frequently test their business continuity, and disaster recovery plans to ensure they are in line with their ongoing operations and effective in the unlikely event of a serious business disruption. Implementing a business continuity and disaster recovery strategy with proper logs that have been tested and well-documented is vital.
f. A rapid return to service is crucial for vital business processes and sub-processes, particularly those that depend on external vendors or other third parties. RSPs should identify these processes and determine backup plans to resume service in the case of failure. The ability to retrieve electronic or physical records essential for business resumption should be addressed. When such records are stored off-site or when the RSP's operations must relocate, care should be taken to ensure that these locations are sufficiently remote from the affected operations to minimize the possibility of both the primary and backup records and facilities being unavailable simultaneously.
g. Investing in continual education and training is also crucial to increase employee knowledge of potential risks and help them develop the skills needed to manage them effectively. Individuals should take precautions such as frequent security audits, reliable backup systems, and training on correct technology usage to reduce technical exposures. Furthermore, it's critical to keep abreast of new risks and technology and to continuously evaluate and enhance risk management tactics.
h. To combat the difficulties of fraud and guarantee consumer protection, RSPs should implement a robust risk management system and suitable information and data security. Sufficient infrastructure and information and data security mechanisms should be set up to prevent and identify fraud. A system for promptly informing the appropriate authorities of any odd events/developments, aberrations, delays, incidents, etc., on a priority basis should be set up. The alerts system is designed to promptly track the various risk occurrences to avoid disruptions.
i. RSPs should identify, monitor, and manage all potential sources of risk emanating from interoperability arrangements before engaging in a link or interface arrangement and on a continuing basis once the link or interface is formed. A connection should have a sound legal foundation that supports its design and provides enough protection to the RSPs involved in the link/interface in all applicable jurisdictions. Credit and liquidity risks that develop due to one another should be measured, monitored, and managed by linked RSPs. Credit extensions between the RSPs should have proper limits and be

fully secured by appropriate collateral. RSPs should identify and manage any potential spillover effects from the default of the linked RSP. If a link has three or more RSPs, each participating RSP should determine, evaluate, and control the risks associated with the overall link configuration.

j. RSPs should have governance arrangements that support the security and effectiveness of management information systems (MIS). A written governance structure that establishes distinct and direct lines of duty and accountability should be present in an RSP's MIS. Owners, relevant authorities, participants, and the public should be aware of these arrangements.

k. Management information systems must adhere to regulatory requirements and important fundamental standards such as ISO 20022. For example, a robust password policy, such as keeping track of password usage and regular password changes, preventing users from reusing the last three passwords, etc., is fundamental. It is recommended to regularly monitor the operating system, database, and application system logs. Regular network scanning and monitoring are necessary to detect Denial of Service (DOS) attacks and other intrusions and spyware. There should be an established mechanism for monitoring, handling, and follow-up of cybersecurity incidents and security breaches.

l. To keep track of the issuing and use of the payment instrument, RSPs may set up a centralized database with direct interaction with their authorized/designated agents where possible. In addition, an RSP can ensure the following conditions:
   - Professionally qualified employees or service providers must audit the source code or application providers must vouch that the application does not contain any embedded malicious or fraudulent code.
   - Logs of applications to integrate the monitoring and management of security-related occurrences in a centralized and coordinated manner.
   - In response to increased rouge apps and phishing attacks, external service providers offer anti-phishing and anti-rouge app services for locating and removing phishing websites and applications.
   - A fraud risk management system must have a procedure for risk-based transaction monitoring or surveillance.
   - Accomplish the recovery time objective (RTO)/recovery point objective (RPO) for the system to recover quickly from cyber-attacks/other incidents and securely resume key operations aligned with RTO while ensuring the security of processes and data is safeguarded.

(ii) Compliance (Legal) Risk Management Guidelines

a. The right policy and practices should be put in place by an RSP to manage compliance risk. The policy must also include a definition of compliance risk, goals for managing compliance risk, and procedures for identifying, evaluating, controlling, and managing compliance risk at all organizational levels. The policy should outline the compliance staff's tasks and responsibilities and the compliance officer's communication techniques. It should also establish the compliance function as an autonomous function within the RSP and clearly outline authorities, roles, and information flow for managing compliance risk at all management levels. The policy can also clearly explain an RSP's accepted level of compliance risk exposure.

b. RSPs should identify potential sources of compliance risk. Every material part of an RSP's operations should have a solid, precise, transparent, and enforceable legal foundation in all pertinent jurisdictions.

Although it can be challenging to quantify compliance risk, it can well be defined, understood, and managed within an RSP's capacity and preparedness to address non-compliance. Reduced exposure to sources of compliance risk, implementing an effective compliance function inside the RSP, and an adequate compliance risk management methodology are all reasonable measures RSPs should take to mitigate compliance risk.

c. The RSP's progress toward achieving compliance goals should also be regularly evaluated, and compliance with internal policies, procedures, internal processes, activities, contracts, and clearly outlined tasks and responsibilities should be verified. Compliance with country policies, laws, regulations, procedures, and legal cases—whether they are new or existing should also be evaluated.
d. With high confidence in all pertinent jurisdictions, the legal foundation should cover each substantial part of an RSP's operations. Contracts, procedures, and rules should be clear, transparent, and compliant with all applicable laws and rules. All applicable countries must uphold these policies, practices, and agreements. It is crucial to explain the legal foundation clearly and understandably for RSP operations to appropriate authorities, participants, and, when applicable, participants' customers. Actions by RSPs under such rules and procedures should be highly certain not to be void, reversed, or subject to delays. RSPs operating in numerous jurisdictions should recognize and reduce any risks from potential legal conflicts between those jurisdictions.
e. To assess each source of compliance risk, RSPs must specify the proper methodology. Several tools are used to determine and evaluate compliance risk, such as evaluating RSP's activities and operations concerning a list of possible risk vulnerabilities. This internally driven procedure frequently uses checklists to determine the advantages and disadvantages of the compliance risk environment.
f. Risk indicators are statistics or matrices that shed light on the compliance risk situation of an RSP. These indicators may include the quantity and/or frequency of legal violations, the frequency of complaints, the number of legal actions that have been initiated, the payment of damages, fines, and court costs, unfavourable court decisions or the number of cases that have been adjudicated regularly, and the frequency of fraud or money laundering activities, whether actual or suspected. These indicators should serve as strong incentives, linking risk to capital and fostering desired growth in the compliance function.
g. While identifying and assessing this risk category, different departments or units are defined according to different risk categories. For instance, the credit function may be outlined according to the risk of improper contract interpretation or a lack of contract enforcement. This exercise can highlight areas of vulnerability and assist in establishing management action priorities.
h. The legal department of RSPs should maintain documentation procedures for all court actions taken against or on behalf of the RSP, accurate information about the RSP's performance in court actions, a list of all court actions with their assessment of the likely outcome of the case, and a list of court actions where outside legal counsel represents the RSP. Additionally, the RSP's legal unit should keep records of the types of claims for which it typically files lawsuits and the cases in which it was sued, substantial compliance risk mitigation measures, restrictions on business with questionable counterparts, limiting exposure to legal interpretations, transparent records of the RSP's shareholders, and records of all decisions made by the regulator(s) regarding the RSP as well as documented correspondence between the regulator(s) and the RSP.
i. Compliance risk can also be assessed using performance indicators such as increased customer complaints, corrective actions against the RSP, or legal actions against the RSP for violating laws and

regulations. Regular legal assessments of various RSP products and services and their pertinent documentation can be used to measure and control compliance risk by ensuring that all contracts adhere to all applicable laws and regulations. This assessment may focus on each transaction separately or consider whether typical forms and procedures are permissible. Routine analysis of certain compliance risk indicators to monitor their compliance risk profiles is critical to provide management people with an early warning signal.

j. RSPs must compile a database of all their legal documents. The category of legal documents, such as contracts, memoranda of understanding, etc., the term of the document's validity, and the department or unit in charge of document enforcement should, at the very least, be included in this database. The database should contain, at a minimum, the definition of the required legal documents. The database should have the legitimacy of the available documentation verified by an RSP's legal expert. The database may also contain the format of standardized contracts for similar RSP products, customers, and other services with third parties, procedures for safeguarding original legal documents, and regular compliance checks.

k. The terms or conditions of each contract should be verified by a legal professional for the RSP. It is important to pay close attention to the steps involved in amending a signed contract. Annexes to any contract are required, as is the due diligence of the RSP's key customers and counterparties, vendors, and outsourced enterprises, and validation of these items by the RSP's legal expert.

l. Internal control systems should provide for the effectiveness of the legal risk management framework and adherence to a set of internal regulations. Checking for compliance with management controls, rules, processes, and procedures regarding the review, treatment, and resolution of non-compliance concerns, as well as reviews of the RSP's progress toward the stated objectives, are just a few examples of key components of this.

m. The compliance function should be independent, have sufficient resources, and be given well-defined tasks. The compliance team, especially the head of compliance, should not be in a position where their other obligations might conflict with their compliance obligations. The head of the compliance department might or might not be in the management team. If the head of the compliance unit is a manager, they should not be in charge of any specific business lines. If the head of compliance is not in the management team, they should report directly to someone in the management team who is not responsible for any specific business functions.

n. The compliance function should ensure regulatory reporting. For a regulated RSP, compliance with the reporting requirements stipulated in various laws, regulations, guidelines, circulars, instructions, and directives is critical.

o. The compliance risk should be considered in the internal audit function's risk assessment methodology, and a programme that evaluates the efficacy and sufficiency of the RSP's compliance function should be implemented. Controls that are appropriate for the perceived degree of risk should be tested.

p. The internal audit and compliance functions should be maintained apart to allow for objective evaluation of the compliance function's operations. Nonetheless, the audit function should alert the head of compliance to any outcomes of the audit that pertain to compliance.

q. The internal audit function should, within the scope of its responsibilities, cover the aspects of compliance risk management, such as confirming that compliance risk management policies and

procedures have been implemented successfully throughout an RSP, evaluating the efficacy of controls for reducing fraud and reputational risks, determining that management personnel takes the proper corrective actions when compliance failures are identified, and making sure that the scope and frequency of compliance failures are appropriately addressed.

(iii) Strategic Risk Management Guidelines

a. In a policy, RSP management personnel should describe the strategic risk, its sources, mitigating measures, and a management strategy. Additionally, the approved tolerance for strategic risk exposure by RSPs must be provided.
b. A qualified board of directors, competent management personnel and staff, ongoing training, a successful risk management system, adequate information access, and the timely and effective introduction of new products or services are all mitigating factors for strategic risk. The strategic risk may present itself in several RSP units if not properly managed, and identifying it may be challenging because it tends to blend with RSP culture. It may also further affect the market position of an RSP, such as a declining target market share.
c. RSPs must have a strategic plan with a clear vision and goals, review and adjust their plans frequently to reflect changing conditions, and ensure all departments work together and communicate effectively to manage strategic risks. This can entail creating frameworks for risk management that recognize potential risks, periodically assess and evaluate progress toward strategic goals, and allocate resources wisely to reduce risk. Furthermore, it is crucial to have robust governance frameworks to guarantee that decision-making procedures are open and accountable.
d. A strategic plan is a written statement of an RSP's mission and long-term objectives, typically covering at least four years. A robust strategic plan must be concise, consistent with goals, adaptable, and responsive to environmental changes. The business breadth, complexity, external environment, and internal variables of the RSP, including its size and resources, should all be considered while developing the strategic plan, operational plans, and budget. In addition, the strategic plan should include an evaluation of the external environment in which an RSP operates and the internal environment, such as the RSP's performance, strategic aims and objectives, risk management system, mission statements, operational plans, and financial projections.
e. The board of directors should ensure that the strategic plan is implemented successfully and evaluated at least once a year. It should also be aware of the market, economic, and competitive factors that affect an RSP. They should obtain fast, accurate, and relevant reports that are useful in the decision-making process. RSP management personnel should actively participate and carefully assess whether business and strategic initiatives are realistic and appropriate based on information. All personnel and departments participating in the strategic planning should cooperate and communicate effectively.
f. The operational plans' objectives should align with the strategic plan, the RSP's overarching goals, and the budgetary allocation. The RSP should establish objectives aligning with its resources, market share, and competitive landscape. Adequate, appropriate, accurate, and timely information will provide a clear understanding of the RSP and its marketplace, which will positively impact the formulation of strategic and business plans and management personnel decisions.

g. To keep track of and make appropriate and consistent plan adjustments in response to changes, RSPs should periodically compare actual performance to the strategic plan. The evaluation must be quantifiable and conducted frequently enough.
h. An effective management information system (MIS) must be in place to monitor strategic risk. By gathering and analysing data, MIS aids in the strategic plan's implementation. RSPs may detect and assess their strategic risk with the help of an MIS, which can also improve employee communication and help to promptly provide the data and reports needed by the RSP board of directors, management personnel, and staff, thus supportive of objectives, goals, and provisions of the services. The type of MIS depends on the complexity and diversity of the RSP's business operations. Furthermore, an effective MIS should be able to gather, store, and retrieve internal and external data, including financial, economic, competitive, technological, and regulatory data and information.

6.2.6 Reputation Risk Management Guidelines

Identifying, evaluating, and controlling possible hazards to an RSP's reputation is important to corporate governance. All of the concerns outlined above can jeopardize one's reputation.

The formality and sophistication of RSPs' reputational risk management framework should be commensurate with the RSP's size and risk profile.

The following guidelines are pertinent to reputation risk management.

a. Identifying the key factors that contribute to this risk. This includes understanding the RSP's values, mission, vision, and the stakeholders' expectations.
b. Identifying the potential exposures that could harm an RSP's reputation. This includes identifying risks related to the services, employee behaviour, relationships with counterparties, regulatory compliance, and other areas.
c. Creating a management plan that outlines how an RSP can manage reputation risks. This includes establishing protocols for addressing negative events or crises, monitoring social media and other sources of information, and developing a crisis communication plan.
d. Establishing clear expectations for ethical behaviour and holding employees accountable for meeting these standards.
e. Communicating openly with stakeholders, responding promptly to feedback and complaints, and demonstrating a commitment to responsible business practices. Working with key stakeholders, including customers, employees, investors, and suppliers, is worthwhile to build trust and address reputation risks. This includes engaging in open communication and seeking input from these groups on improving the RSP's reputation.
f. Regularly monitor and measure an RSP's reputation, including tracking social media sentiment, media coverage, and customer feedback. This will help the identification of potential reputation risks and address them proactively.
g. Continuously improve RSP's reputation risk management programme by establishing a process for evaluating the RSP's reputation risk management programme and making improvements as needed. This includes conducting regular assessments, seeking stakeholder feedback, and updating the programme.

An RSP can proactively and systematically identify, assess, and manage risks by adhering to the above-mentioned risk management guidelines. This can aid in reducing potential losses, safeguarding the RSP's brand, and ensuring regulatory compliance. Although there is no one-size-fits-all strategy for risk management, an RSP can customize these guidelines according to its requirements and circumstances. By doing this, the remittance markets can be safe and sound, with reliable remittance services.

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