IFAD
Investing in rural people

Financing Facility
for Remittances

cenfri

Co-funded by
the European Union

IFAD Remittance Innovation Toolkit

In implementation of

PRIME
AFRICA

Authors

Liebe Burger, Lezanne Anderson,
Christine Hougaard, Masiiwa Rusare,
Barry Cooper
With support from Nora Hattar
and Yuvir Naidoo

Cenfri South Africa

The Vineyards Office Estate
Farm 1, Block A
99 Jip de Jager Drive
Bellville, 7530, South Africa
PO Box 5966
Tygervalley, 7535, South Africa
Tel: +27 21 913 9510
Email: info@cenfri.org
www.cenfri.org

IFAD

Financing Facility for Remittances
Via Paolo di Dono, 44
00142 Rome, Italy
Tel: +39 06 54591
Email: ifad@ifad.org
remittances@ifad.org
www.ifad.org

Acknowledgements

The authors are grateful for the valuable feedback provided by Amal Express Money Transfer, Ecobank Uganda, Ecobank Ghana and Wizall Money on the content and testimonials of their experience on the project.

The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the International Fund for Agricultural Development of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. The designations “developed” and “developing” economies are intended for statistical convenience and do not necessarily express a judgement about the stage reached by a particular country or area in the development process.

Cover photo: ©Adobe Stock/Rido

Table of contents

List of tables

List of figures

List of boxes

Acronyms

AFI	Alliance for Financial Inclusion
AML	anti-money laundering
API	application programming interface
BoU	Bank of Uganda
BVN	bank verification number
CDD	customer due diligence
CFT	combating the financing of terrorism
CGAP	Consultative Group to Assist the Poor
CPF	countering proliferation financing
CRG	Co-operation Review Group
ECDD	enhanced customer due diligence
eKYC	electronic know-your-customer
EU	European Union
FATF	Financial Action Task Force
FFR	Financing Facility for Remittances
FIC	Financial Intelligence Centre
FIU	Financial Intelligence Unit
GDP	Gross Domestic Product
GPS	Global Positioning System
GSMA	Groupe Speciale Mobile Association
ID	identification or identity document
IFF	illicit financial flows
IFAD	International Fund for Agricultural Development
IMF	International Monetary Fund
IMTO	international money transfer organization
IP	internet protocol
IPRS	integrated population registration services
IT	information technology
JPEG	Joint Photographic Experts Group
KPIs	Key performance indicators
KYA	know-your-agent
KYC	know-your-customer
MAP	making access possible
M&E	monitoring and evaluation
MER	mutual evaluation report
ML	money laundering
NIC	network interface card
NRA	national risk assessment
NRB	national registration bureau
OECD	The Organization for Economic Cooperation and Development
OFAC	Office for Foreign Assets Control
OTC	over-the-counter
OTP	one-time PIN
PEP	politically-exposed persons
PF	proliferation financing
PIN	personal identification number
PNG	portable network graphics
PRIME	Platform for Remittances, Investment and Migrants' Entrepreneurship
RAI	Remittance Access Innovation programme

RBA	risk-based approach
RSP	remittance service provider
SDN	specially designated nationals
SGR	system-generated receipts
SIM	subscriber identity module
SMS	short message service
TBML	trade-based money laundering risk
TF	terror financing
TPDD	third-party due diligence
UAT	user-acceptance tests
UNCDF	United Nations Capital Development Fund
UNHCR	United Nations High Commissioner for Refugees
US	United States
US$	United States Dollar

Glossary

Agent network
Agent networks are comprised from independent, small-scale dealers and other shops, or they can be a part of an existing distribution network like post offices or retail chains. Depending on current laws and regulations, agents can frequently carry out simple financial operations on behalf of banks, including withdrawals, deposits, money transfers and payments (CGAP, n.d.)

AML/CFT/CPF
Refers to anti-money laundering (AML), combatting the financing of terrorism (CFT), and countering proliferation financing (CPF). Accountable Institutions and regulators normally take measures or activities aimed at combating money laundering, terrorism financing and proliferation financing

Collaborative KYC/CDD systems
Collaborative KYC/CDD systems involve multiple entities working together to streamline and improve the efficiency of verifying customer identities and conducting due diligence checks (CGAP, 2018)

Compliance
Refers to the application of the particular regulatory obligation, including the legal framework and methods of enforcement, and the presence, authority and protocols of relevant agencies (FATF, 2023).

Compliance obligations
The legal requirements an organization must comply with and non-mandatory requirements that an organization chooses to commit to (ISO, 2019).

Customer due diligence (CDD)
Customer due diligence is the process used by financial institutions to collect and evaluate relevant information about a customer, potential customer and related transactions to curb money laundering, terrorism financing and proliferation financing

De-risking
De-risking is the practice of financial institutions terminating or limiting their business relationships with clients or client categories to avoid rather than manage risks (FATF, 2014).

Digital identity
This refers to utilizing electronic methods to assert and validate an individual's official identity either in online (digital) or in-person settings, with different levels of assurance (FATF, 2020)

Digital foundational identity
This refers to the government or authority issuing ID (for example birth certificate, national ID) in digital form.

Foundational identity
A foundational identity is an identification normally issued by a government or authority that provides universal coverage within the population. It identifies a holder and then gives them general access to public and private sector services. Examples include birth certificates, national identity, etc.

Functional identity
A functional identity is an identifier that identifies a holder and gives them access to specific services or transactions, e.g. financial services, social programmes and transfers, tax administration, voting and more. Examples include voter IDs for voting, health and insurance cards for insurance access, tax ID numbers, ration cards for access to rationed food and driver's licenses. However, in some cases, these can be used for additional purposes other than those for which they were designed (The World Bank, 2021). For example, using a voter's card for financial services access.

Identity proofing
Identity proofing answers the question, "Who are you?" and refers to the process by which an identity service provider (IDSP) collects, validates and verifies information about a person and resolves it to a unique individual within a given population or context. It involves three actions: (1) collection/resolution; (2) validation; and (3) verification (FATF, 2020).

Know-your-customer (KYC)
Know-your-customer (KYC) is a business concept centred around knowing (through identifying and verifying) one's customers and their transactions for AML/CFT/CPF purposes. It is a key component of a more comprehensive ongoing customer due diligence programme.

Principles-based approach
A principles-focused rules-based approach fixates on compliance inputs by rule.

Proxy identity
A proxy identity, or alias, is an identifier or collection of identifiers and attributes that can uniquely identify an individual or link to a foundational identity (if one exists). This can then be used by the holder to access public and private services (World Bank, 2021).

Regulatory sandbox
A regulatory sandbox is a system established by a financial sector regulator to enable businesses to test new and innovative products, services, or business ideas in a controlled environment for a limited time while being closely supervised by the regulator (CGAP, 2017). Sandboxes create a regulatory safe space for innovators to test their products by temporarily reducing or waiving regulatory requirements (either explicitly or implicitly) while imposing specific safeguards to ensure that consumer protection is not compromised (Cenfri, 2018).

Remittance service provider (RSP)
A remittance service provider is an entity that facilitates the transfer of money between customers or businesses for a fee. This could be local or cross border.

Remote identity proofing
Remote identity proofing is the process by which an identity service provider (IDSP) collects, validates and verifies information about a person and resolves it to a unique individual within a given population or context. It is a sophisticated method of identity verification that allows users to validate their identities remotely (FATF, 2020)

Remote onboarding (also referred to as non-face-to-face onboarding)
Remote onboarding refers to introducing a new client to a product or service while both parties are not in the same physical location, or conduct activities by other, often digital, means (FATF, 2020).

Risk assessment
Risk assessment is the process of identifying, assessing, and understanding money laundering and terrorism financing risks for an institution or jurisdiction (FATF, 2023).

Risk-based approach
Risk based approach refers to the process of risk mitigation that ensures that risk control measures and activities are informed by and commensurate to identified risks. It involves identifying, assessing, and understanding the risks one faces and applying control measures aligned with the identified risks (FATF, 2014).

Rules-based approach
A rules-based approach is an approach to managing risks that relies on specific rules to manage ML-TF-PF risks. irrespective of the nature and level of risks. This approach has been deemed ineffective in mitigating ML and TF risks as it is often ticking box and doesn't address underlying ML, TF, PF risks. Resultantly FATF has mandated a risk-based approach instead. Risk based approach focuses attention and resources on key and significant risks and requires appropriate controls.

User acceptance testing
Refers to a final stage in software development involving real-world testing by the intended audience to identify any problems that need to be corrected before the software goes live (Cambridge Dictionary, n.d.). It is also referred to as application testing or end-user testing.

This is an interactive document. Clicking on the in-text title headings and references to supporting materials will navigate you directly to the content in reference.

Executive summary

Access to remittances is indispensable for one in every eight people worldwide. Remittances are a lifeline for millions, providing access to food, healthcare, education, and funds to grow small businesses and access credit, particularly in less developed economies. In doing so, they contribute directly to the United Nations Sustainable Development Goals (SDGs). Due to the agility and ease with which remittances can be provided, they have been mobilized as a vehicle for reaching, supporting and increasing the financial resilience of vulnerable populations. It is estimated that over 50 per cent of remittances globally are sent to rural areas where the most vulnerable and food-insecure populations live (IFAD, 2023).

However, barriers to remittance access remain. According to the World Bank, sending remittances in Africa is expensive, costing an average of 8.5 per cent of the amount being transferred, compared to an average of less than 6 per cent globally (United Nations, 2022). But cost is only half the battle. Remittance receivers using official channels, such as remittance service providers (RSPs), are often faced with a variety of burdensome know-your-customer (KYC) and customer due diligence (CDD) requirements, such as the need to present proof of address, or to receive remittances in person despite living in an area without access to a branch. Many of these requirements are rooted in legacy and rules-based regulations or in RSPs' over-compliance with regulations. These practices prevail despite Financial Action Task Force (FATF)[1] guidance on flexible identification, KYC and CDD requirements, which aim at reducing unintended consequences such as financial exclusion and de-risking.

[1] The FATF is a global standard setting body on Anti Money Laundering and Countering Terrorism Financing (AML-CFT). It developed and oversees the implementation of 40 recommendations/ standards on AML-CFT. For mor information please visit www.fatf.org

Barriers are a development challenge and stifle commercial opportunity. As long as these barriers remain in place, they impact remittance receivers' access to livelihood opportunities and push people into informal channels. If these barriers can be overcome, RSPs have a commercial opportunity to unlock a previously untapped customer base. Thus, there is a clear development as well as commercial imperative for enhancing remittance access through KYC and CDD innovation.

Bridging the gap: a toolkit to enhance remittance access and growth. There is currently limited to no guidance available to RSPs on how to assess a regulatory regime to identify opportunities for innovation in KYC and CDD processes to enhance remittance access. Building on the experience of IFAD under the Remittance Access Innovation (RAI) programme rolled out in seven African countries, this toolkit provides practical guidance for regulators and RSPs on how to **(1)** assess national regulatory environments; **(2)** analyse contextual realities, highlighting key risks and opportunities for innovation; and **(3)** plan, implement and measure innovative interventions to address KYC and CDD barriers to remittances.

Financial sector regulators and RSPs are the primary audience of this toolkit, each standing to benefit from it:

- **Financial sector regulators and supervisors** can enhance their country's AML/CFT regimes, mitigate the de-risking of customers and institutions, align more effectively with FATF and other international best practices, drive down remittance costs and strategically leverage remittances to actively contribute to national objectives such as fostering economic growth, building financial inclusion and supporting livelihoods, thereby contributing to the SDGs.
- **Remittance service providers** are equipped to retain their existing customer base, capitalize on unexplored target markets, broaden their revenue streams, reduce time and cost spent on compliance arising from onerous KYC and CDD processes, and harness data to craft novel products and services.

What you can expect: practical guidance on innovating on compliance and enhancing remittance access. This toolkit provides practical guidance for financial sector regulators and RSPs to step into the innovation space and break down barriers to remittance access. It does so by delineating the steps for (1) conducting a regulatory assessment to understand the parameters for innovation; and (2) developing innovative interventions to enhance remittance access, looking at **five key interventions:**

The starting point: regulatory assessment

Given the challenges faced by an RSP, innovation starts by **assessing the regulatory regime** within which remittance access innovation takes place:

- **For RSPs,** there is constant pressure to remain compliant while innovating to stay relevant and grow. This toolkit helps RSPs do both by providing guidance on how they can conduct a regulatory assessment to better understand their compliance obligations, to map the regulatory parameters within which they can innovate and to identify areas for innovation.
- **Financial sector regulators**, in turn, need to assess the effectiveness of the regulatory regime to ensure it fits the local context and supports inclusion, while keeping up with international standards and best practice on financial integrity. In a separate deep dive on regulatory assessment for regulators, this toolkit provides practical guidance on how to (1) assess the effectiveness of the regulations, identify strengths and consider which regulations could be acting as barriers to remittance access; (2) identify international standards and best practice, as set by The Financial Action Task Force, to update, upgrade and enhance the regulatory regime through regulatory reform or tools like guidance papers; (3) make practical changes to regulations and/or compliance instruments; and (4) understand and guide the realities of the remittance market.

This first step then serves as the foundation for implementing remittance innovations.

How-to guide for five core remittance innovations

The rest of the toolkit focuses on practical guidance for RSPs on how to **develop an innovative intervention** to enhance remittance access. In doing so, it also provides insight into the remittance market for financial sector regulators by highlighting the typical barriers faced by RSPs.

For each innovative intervention, the toolkit outlines the benefits and costs for the organization and provides a list of requirements and a step-by-step guide for implementation and for measuring the success of the intervention. It concludes by sharing lessons from RSPs that have implemented this intervention.

The interventions in a nutshell. The table below outlines the essence of each of the five innovative interventions:

The intervention	What the toolkit covers	Benefits of this intervention
1. Conducting a **risk assessment and developing proportionate responses** **Purpose:** to strengthen the robustness of the organization's risk assessment and/or identify areas of opportunity specific to your business	Guidance on how to identify the inherent risks and the key drivers of these risks; set up a risk assessment framework and import data to it; update the organization's risk appetite; leverage the updated risk assessment matrix to enhance the business; and build internal team capacities. It also includes a template on how to set up **a risk assessment matrix**.	• Craft a comprehensive, validated and up-to-standard proportionate risk matrix • Reduce compliance resources required and bring down the risk of fines • Identify areas for further innovations, such as new remittance corridors and customer segments
2. Developing a **digital ID database** **Purpose:** to serve those customers who have forgotten, lost or damaged their IDs.	Guidance on how to collect ID copies, technical support for setting up a digital ID database, guidance on the design and user experience, security support, and guidance on how to roll out and assess a pilot. This discussion also includes templates for a **digital ID database interface**.	• Reduced cost of compliance • Improved customer satisfaction due to increased convenience • Enhanced digitalization
3. Developing **remittance customer profiles** **Purpose:** to enable once-off KYC for over-the-counter customers, strengthen the track record of financial transactions and create the base for identity proofing.	Guidance on how to set up a customer profile platform and integrate it with a digital ID database or third-party system, setting up the customer and staff interface, the required security standards and procedures, and on how to train staff and sensitize customers about the process changes.	• Reduced fraud • Increased visibility of the KYC process conducted by cashiers • Ability to identify new opportunities to target customers for affiliate products based on their transaction behaviour
4. Replacing manual money transfer forms with **printed receipts** **Purpose:** to better serve semi-literate and illiterate customers who cannot access their remittances without support.	Guidance on how to identify and add missing fields to the printed receipt, to replace the manual form, train staff and sensitize customers on the system changes. This includes an **actual example** of the information added to the printed receipt and a **revised customer journey**.	• Increased customer retention • Reduced chances of error • Improved customer experience due to faster turnaround time • Reduced cost of compliance specifically by reducing paper-based administration
5. Improving the agent risk-assessment process and the **agent onboarding policy.** **Purpose:** to expand the agent network to better serve hard-to-reach communities.	Guidance on how to understand the needs of agents, conduct a regulatory and risk assessment of an agent's business and how to conduct a pilot for the intervention. The step-by-step implementation guide includes a template for an **agent risk assessment matrix**.	• Expansion of agent network • Enhanced risk management for agents • Potential to onboard more customers • Ability to identify new opportunities where agents can support business expansion (e.g. value-added services)

Tools to integrate into compliance and business practices. The best practices, country examples and real-life lessons captured in this toolkit speak to the remittance landscape as experienced on the ground, and the tips, guides, and step-by-step support draw from interventions that have been tried and tested by financial sector regulators and RSPs active in the African remittance market. For systemic and sustainable change, this toolkit should be integrated into the reader's institutional practices and processes on an ongoing basis. It is designed to be used by regulators and RSPs across the development scale, to support continued progress towards enhancing remittance access and supporting sustainable market growth.

Introduction: Why a remittance innovation toolkit?

A guide to unlocking remittance access innovation for livelihoods and growth. Financial sector regulators and RSPs are in an ideal position to drive financial inclusion and strengthen financial integrity through innovation. Doing so can meaningfully enhance the livelihoods of low-income and rural households, thereby contributing to the SDGs and unlocking substantial commercial and growth opportunities[2]. However, there is little support and guidance available to help them address barriers to remittance access, specifically those related to KYC and CDD.

Meeting the need: increased demand for innovation support based on the Remittance Access Innovation (RAI) programme. The need for this toolkit was identified during IFAD's work under the RAI programme – see the box below for a brief overview. RSPs and regulators expressed the need for leveraging innovation to achieve strategic inclusion, innovation and integrity objectives. The toolkit provides practical step-by-step guidance for RSPs and regulators on how to enhance remittance access and stimulate growth. To ensure that it is practical, it includes several tips, templates and check-in points.

Background: the Remittance Access Initiative. In 2020, under the Platform for Remittances, Investment and Migrants' Entrepreneurship (PRIME) Africa Program, financed by the European Union, IFAD conducted remittance diagnostic studies in seven PRIME countries, namely The Gambia, Ghana, Senegal, Kenya, Uganda, South Africa and Morocco. These diagnostics revealed that KYC and CDD practices can act as a key barrier to remittances, specifically for low-income rural households and women. To address this, Cenfri and IFAD launched the Remittance Access Innovation (RAI) programme in 2021 to enhance remittance access for low-income rural households and women in these seven countries. This programme provided technical assistance to a total of thirteen RSPs and five regulators. By 2023, the programme had removed KYC and CDD barriers for 358,305 customers and 44,689 transactions. The technical assistance provided under the RAI had far-reaching benefits for RSPs and regulators, and the program generated significant interest in African remittance markets.

[2] As explained further in **Deep dive 1: Leveraging remittances to bolster growth in Africa**.

This toolkit is structured as follows:

- **Chapter 1: Choosing a fit-for-purpose intervention.** A remittance innovation is most effective if it addresses an actual challenge to serving vulnerable groups with remittances as experienced on the ground. Understanding the challenge to be addressed in a specific context, and choosing an appropriate intervention, accordingly, forms the point of departure for any RSP engaging with this toolkit. Chapter 1 identifies **five potential innovative interventions** to respond to specific challenges as identified through the RAI, which then form the basis for the rest of the toolkit.

- **Chapter 2: Conducting a regulatory assessment.** Regardless of which innovation an RSP wants to implement, the starting point is to conduct a regulatory assessment, as the regulatory framework sets the parameters within which innovation is permitted. This chapter provides a step-by-step approach to conducting a regulatory assessment. **For RSPs**, doing a regulatory assessment is essential to ensure that they operate within the regulatory framework, that they identify the best opportunities for innovation, and that they highlight any regulatory stumbling blocks when embarking on a given innovation. **For regulators**, in turn, a regulatory assessment is key to align with international best practices and make progress towards inclusive integrity goals. Chapter 2 is accompanied by an Appendix to provide additional reference materials.

- **Chapter 3: Implementing remittance access innovations for RSPs.** To support RSPs in using innovation related to KYC and CDD to grow their business while enhancing remittance access, this toolkit provides a step-by-step guide on **the five identified innovative interventions.** For each, it details the reason for the intervention and its benefits for RSPs, identifies the resources needed for implementation, and provides a practical implementation guide. Finally, it outlines how to measure the impact of each intervention by looking at case studies and examples, developing key performance indicators, exploring data collection and analysis, and discussing staff training and customer sensitization.

- **Chapter 4** concludes by discussing the final steps for securing systemic, sustainable, and inclusive growth for RSPs and remittance markets.

Supplementary deep dives. The main text is supplemented by four hyperlinked **deep dives** for further detail on specific topics.[3] Each deep dive provides complementary information or additional practical support. These are:

Chapter reference	Deep dive	Summary
Introduction	Deep dive 1: Leveraging remittances to bolster growth in Africa.	Exploration of the value of remittances in Africa for economic growth and financial inclusion, and of the structural and market barriers that inhibit access to remittances that this toolkit aims to respond to.
Chapter 1	Deep dive 2: Developing and implementing your own innovative intervention to address KYC and CDD barriers.	Step-by-step guide for RSPs on the process of how to develop and implement an innovative intervention of their choice to address KYC and CDD barriers, over and above the five interventions showcased in this toolkit.
Chapter 2	Deep dive 3: A guide for regulators to assess regulations against inclusive integrity goals and best practices.	Guidance for regulators on how to assess their regulations by providing practical steps for defining inclusive integrity goals, aligning with international best practice, amending regulatory frameworks and measuring the success of inclusive integrity goals. This deep dive is also useful for RSPs who wish to better understand the mechanisms influencing regulatory change.
Chapter 3	Deep dive 4: A practical addition to the risk assessment intervention	Illustrative example of how to set up a risk assessment matrix, along with step-by-step descriptions of how to tailor the risk assessment matrix to an RSP's unique context, as well as broader considerations for following a proportionate approach to risk.

Two key audiences. This toolkit aims to benefit RSPs and financial sector regulators and supervisors as the primary audiences:

- For **RSPs**, this document sets out practical guidance illustrated by examples on how to innovate and better align with national regulations, as well as concrete steps to remove KYC and CDD-related barriers that are hindering remittance access. Implementing these innovations can help to retain their existing customers, increase their customer base, increase their revenue stream, save on the cost of compliance and enhance their operations. It can also help them to harness data to craft novel products and services.

- **Financial sector regulators and supervisors** can use the nuanced view of the remittance landscape and compliance barriers faced by RSPs as outlined in this toolkit to enhance their respective country AML/CFT regimes and mitigate de-risking of both customers and institutions.[4] In so doing, the toolkit provides them with a how-to guide to align with international standards and best practices as inclusively set by the FATF and to better engage with their respective markets to identify challenges and opportunities for innovation. Ultimately, this will help drive down

[3] Further supplementary information is provided in the Appendixes, which relate to specific chapters of the toolkit. You can navigate to them here.

[4] It also provides insight on the tools that regulators can use to enhance innovation, such as the Regulating For Innovation Toolkit. See the deep dive three discussion on best practices for more.

remittance costs and actively contribute to national objectives such as fostering economic growth, building financial inclusion and supporting livelihoods. Finally, the toolkit creates an opportunity for regulators to set the standard for innovation going forward.

Zooming in on the beneficiaries of the toolkit.

TABLE 1: WHO THIS TOOLKIT IS FOR

Remittance Service Providers	Financial sector regulators and supervisors
This toolkit is relevant **to all types of RSPs**, including but not limited to banks and financial institutions, money transfer operators, online payment platforms, foreign exchange bureaus, digital wallet providers, postal services and fintechs.[5] **Relevant departments within the institutions** include the business development department, the compliance department and the IT department.	The relevant **financial sector regulators** are central banks and non-bank financial regulators, which set the regulatory parameters within which RSPs can operate and innovate, and **financial supervisors**, including financial intelligence units, who evaluate the compliance of financial institutions with laws and regulations. **Relevant departments within the respective institutions** include the payment system department, the financial stability department, the technology and innovation and the financial inclusion unit. Other departments to consult include the consumer protection unit and banking supervisory department. Note: departments differ across financial sector regulators and supervisors, therefore it may be important to identify departments or units with similar mandates.

Building on a legacy of tried and tested knowledge to enhance remittance access. This toolkit has been built upon a decade of experience, first principles thinking and learnings from interventions, other toolkits and innovations tested in real environments. The strategies and interventions based upon this body of knowledge have resulted in countries being removed from the FATF grey list, set on a sustainable inclusive integrity path and transforming into regional leaders in inclusive integrity. The learnings come from KYC and CDD barriers being removed for millions of consumers whilst enhancing the effectiveness of their countries in the fight against money laundering (ML), terror financing (TF) and proliferation financing (PF). The toolkit consolidates these learnings and makes them available as a public good for the benefit of RSPs and regulators. Stakeholders have over the years tried and tested several innovative interventions to get to a shortlist of solid innovations which are reliably able to add value to institutions, markets and regulatory environments as presented in this toolkit. That legacy is now available to all as a public good and merely requires the reader's diligence and dedication to achieve quantifiable goals.

[5] Note: It will be essential for each RSP using this toolkit to carefully apply the regulatory assessment (covered in chapter 2) to define their own regulatory parameters and innovate within those.

1

Choosing a fit-for-purpose intervention

To develop fit-for-purpose interventions, it is crucial to first establish the context by understanding what the specific compliance barriers to remittance growth are for any specific RSP. Based on the RAI programme, many of the barriers to sending and receiving remittances are rooted in RSPs' compliance processes. In most jurisdictions, either through law or regulations reflecting the FATF recommendations, RSPs are required to identify[6] and verify a customer's identity and assess their risk level before establishing a relationship as well as throughout the relationship. This is done through KYC and CDD[7] processes, respectively. These processes are essential for combatting money laundering, terror financing and proliferation financing (ML/TF/PF). However, these processes can also create barriers to remittance access (IFAD, 2023).[8] These barriers have a myriad of negative consequences, including but not limited to excluding people from accessing their remittances, increasing the cost of compliance and negatively impacting the customer experience. This is especially the case for vulnerable groups such as low-income, rural households

[6] Subject to product and channel controls and mitigation as the customer's inherent risk profile emerges.

[7] KYC entails identifying and validating consumers as well as their business intents as part of a more extensive ongoing customer due diligence (CDD) effort. The purpose of KYC procedures is to proactively screen clients for risk indicators related to money laundering, terrorism financing, corruption, and fraud (Society for Worldwide Financial Telecommunications, n.d). CDD is a procedure that financial organizations employ to gather and assess pertinent data about a current or prospective client. It looks for anything that could put the financial institution at risk from the customer. Involves monitoring, risk analytics, and behavioural aspects of the customer and/or product in relation to the data gathered in KYC. If the customer profile changes, additional information may be required, such as proof of income or profession, in which case increased due diligence may be necessary (Society for Worldwide Financial Telecommunications, n.d).

[8] This was illustrated by the Remittance Access Initiative (RAI) recently implemented by the International Fund for Agricultural Development's (IFAD) Financing Facility for Remittances (FFR) and Cenfri (IFAD, 2023).

and women, who are often disproportionally impacted. These barriers can arise in three interrelated ways:[9]

- **Outdated and overly complicated regulations** that do not align with international standards and best practices set by the FATF and the relevant updates thereof. These standards include the most up-to-date approaches for applying a risk-based approach (RBA), requirements for CDD and recordkeeping. Misaligning with these best practices, or maintaining outdated practices, risks poor integrity outcomes, financial exclusion and de-risking. Thus, the first step in the innovation journey is to conduct a regulatory assessment – see chapter 2.

What is de-risking?
It is the practice where financial institutions choose to terminate or limit business relationships to avoid risk rather than managing it (FATF, 2014).

- **RSPs' over-compliance**. The key drivers of compliance in most jurisdictions include what is in the hard laws and regulations, non-binding agreements, declarations (soft law) as well as how stakeholders perceive the intent of the law and its implementation (spirit of the law), among others.[10] All of these shape supervisors' or institutions' actions and responses. This means that in some jurisdictions over-compliance is hard coded in laws and regulations (for example through requesting more information or documents than what the FATF guidelines require, such as proof of address), while in others it is due to the use of soft law (non-binding requirements and agreements between institutions and regulators) that requires market players to do more than what is in the law. When RSPs over-comply, by implementing strict requirements that are at times not required by law or adapted to their jurisdiction, it imposes a barrier and results in financial exclusion and related risks to the financial sector.
- **RSPs implementing KYC and CDD through outdated practices.** In many cases, it is not the KYC and CDD that cause the barrier, but rather how these are implemented. For example, many RSPs are still verifying customer information via manual, hand-written forms despite already having this information on their digital back-end systems. This process risks excluding semi-literate customers and increasing the cost of compliance (in terms of time spent and in terms of using paper-based forms). Innovations in KYC and CDD practices are key in addressing this challenge.

To identify the barriers stemming from their own practices, and to assess the effectiveness and cost of their compliance processes, RSPs can assess whether their customers can easily access their remittances, the documentation requirements they impose on them, and how they risk rate their customers.[11]

[9] For more on the underlying drivers of these reasons, please see the Inclusive Integrity Toolkit.

[10] For more information on the drivers of over compliance behaviour please visit: Conservative compliance behaviour.

[11] For further reading on market-related barriers to remittances, see the Cenfri report here, or the IFAD remittance market diagnostic reports here.

Key questions to ask yourself as an RSP representative

- Is my organization requesting any form of ID for a remittance transaction even if it is not required by law? (for example, proof of address)
- Are customers not coming to collect their remittances? If so, why not? Are they illiterate? Do they live too far away? Is there a language barrier? Or may there be a challenge related to the documentation that they must show?
- Are customers complaining about having to share too much personal information (specifically information that's not required by law)?
- Are customers complaining of long waiting times and inconvenient processes?
- Are customers unable to access their remittances because they forgot, lost, or damaged their ID, despite being a loyal customer/having used your remittance services before?
- Are my current KYC and CDD controls effectively mitigating money laundering, terrorism financing and proliferation financing risks or just compliance risks?
- Do my organization's AML/CFT/CPF measures inappropriately hamper the achievement of financial inclusion objectives?
- Are my organization's AML/CFT/CPF measures effective and efficient in achieving inclusive integrity objectives?

Answering yes to any of these questions indicates that the RSP is experiencing barriers to remittances within its organization. An example of a barrier would be requesting proof of address as a form of verifying a customer's identity, where it is not required by law[12] and where a customer has already been verified through a robust ID.

The next step is to devise an innovative intervention to address the key barrier(s). Based on the barrier(s) identified, an RSP can then develop an innovative intervention to address the relevant barriers and start the process of implementing it in their organization. Table 2 below lists some frequent KYC and CDD-based challenges that are inhibiting remittance access in Africa. Alongside each is an innovative intervention that was implemented under the Remittance Access and Innovation programme **(RAI)** to address it. These interventions will be unpacked further in chapter 3.

[12] For example, in South Africa, some financial institutions still request proof of address for persons to open a bank account despite it no longer being required by law (Cenfri, 2020). Although its normally requested together with other identifies such as national identity document, it normally becomes a key determining factor or access especially for low income and rural customers with difficulty to prove address. In addition, proof of address is not a reliable identifier, is costly and time-consuming for RSPs to verify as well as being superfluous when a client has already been verified through a national ID.

TABLE 2: CATEGORIES OF INTERVENTIONS DISCUSSED IN THIS TOOLKIT

Challenge identified	Intervention category	Solutions explored in this toolkit
Lack of/limited data-driven risk assessments resulting in incorrectly rating low income and rural households as high-risk and potentially excluding them from transacting	**Risk assessment and proportionate response**	Using data driven risk assessment and re-rating to measure and understand the real risk posed by low income and rural households plus the financial products used and introduce proportionate risk mitigation measures.
Increasing cases of fraud due to poor tracking of customer transaction behaviour, resulting in increased cost due to incorrect or duplicate pay-outs and compliance investigation costs	**Identity proofing**	Developing a functional digital ID database. Developing remittance customer profiles
High level of rejected- and incomplete transactions due to semi-illiterate customers not being able to complete the manual, paper-based money transfer forms required to collect remittances. This also includes other inconvenience factors such as long queues, crowded front office and people leaving before filling in the forms.	**Replacing manual forms with printed receipts**	Digitising the process and relying on information already available in the RSPs system. Thus, replacing a money transfer form with printed receipts.
Limited physical access points especially in rural areas, reducing the customer base that can be served	**Rural agent onboarding**	Improving the agent risk-assessment process and the agent onboarding policy to increase the number of agents in a risk appropriate manner.

Exploring alternative interventions. The interventions discussed above and explored in chapter 3 may address some of the most common challenges that an RSP faces. However, they may not address all challenges. If you want to develop an alternative intervention that's fit for your specific purposes, see **Deep dive 2: Developing and implementing your own innovative intervention to address KYC and CDD barriers**. This deep dive provides a step-by-step guide on the process of how to develop and implement a tailored innovative intervention to address KYC and CDD barriers specifically by going through the innovation journey.

2

Conducting a regulatory assessment

Understanding the regulatory environment and parameters within which innovation can take place is an essential precursor for an RSP to develop any innovative intervention to enhance remittance access and/or improve business operations. This chapter focuses on how RSPs can assess their national and regional regulations and, from there, extract relevant insights and opportunities to draw the regulatory parameters within which they can innovate and explore innovation opportunities. This chapter is structured as follows:

- Sub-section 2.1 **Relevant regulations** to review for understanding the remittances regulatory landscape
- Sub-section 2.2 **Guide for RSPs to conduct a regulatory assessment** to understand their scope for innovation within the regulatory parameters.

> **A must-read for regulators as well**. This chapter is also important for regulators, as it provides a completeness check of what's needed to enable an innovative environment for remittances. Sub-section 2.1 helps a regulator to identify areas to enhance inclusive integrity and sub-section 2.2 shows them the process that RSP compliance teams go through to understand the regulatory parameters within which they need to operate. Having this understanding is important for meaningful two-way engagement between the regulator and the market.
>
> Beyond spurring RSP innovation, it is also important for regulators to assess their own regulatory framework against global inclusive integrity best practices. **Deep dive 3: A guide for regulators to assess regulations against inclusive integrity goals and best practice** offers guidance specifically for regulators on how to conduct their own regulatory assessment. This deep dive offers practical steps for defining inclusive integrity goals, aligning with international best practices, amending regulatory frameworks and measuring the success of inclusive integrity goals. RSPs who wish to better understand the mechanisms influencing regulatory change will also benefit from reading this section.

2.1 Which regulations are relevant to review?

Three core types of legal instruments shape the regulatory landscape. When undertaking regulatory analysis, it is important to understand the difference between the types of legal instruments that shape the regulatory landscape, and how these different types should be read and approached when considering innovating around KYC and CDD. These legal instruments include:

- **Statutes or acts.** These are pieces of legislation usually passed by a national legislative body having the force of law. Ideally, statutes should formulate legal principles at the strategic level. Therefore, these set the foundation. To use a sports analogy: they can be understood as the football field – the structure or parameters within which operators play.
- **Regulations.** These enable the implementation and functioning of the legislative framework. Continuing with the sports analogy, these set the rules for the game, they must be complied with to operate, or play, in the field.
- **Guidelines or guidance.** These represent authoritative statements issued by government agencies to inform the public of policies to provide clarity on interpretation. Using the above sports analogy, these are the referees: they indicate how the regulations are to be interpreted and implemented on the field and can even give case-by-case assistance.

For RSPs, Acts are the foundation for the market, the regulations are those that they must comply with to be operational, and the guidelines – which offer the most practical support – guide on how they can comply with regulations as well as where there is a scope to innovate and develop a unique strategy and competitive edge.[13]

Start the regulatory assessment by collecting the right documents. Regulatory frameworks (which consist of the acts, regulations and guidelines in a single jurisdiction) differ significantly worldwide. However, there is some consistency in the types of content that need to be reviewed to gain an understanding of the remittances regulatory landscape. The table below shows the typical legal instruments to list, collect and review when conducting a regulatory assessment:

[13] Further information about what each of these legal documents entails as well as the sources for their definitions, can be found in Table 29 of the Appendix.

TABLE 3: LEGAL INSTRUMENTS TO REVIEW WHEN CONDUCTING A REGULATORY ASSESSMENT

Relevant instruments	What to be on the lookout for
Acts	
Anti-Money Laundering Act	An AML act sets out a country's vision, understanding, and expectations regarding money laundering and terrorism financing. It also sets out reporting requirements for institutions as well as measures to address money laundering and terrorism financing, among others. Note: also search for amendments to the Act for updated requirements which supersede the original version
National Payment Systems and Services Act	This Act provides information on the management, administration, operation, regulation and supervision of all payment systems in the country.
Other Acts, e.g. Banking Acts, Central Bank Acts	It is crucial to understand the legislation that forms the mandate upon which regulations and licenses can be issued. This is to ensure that licensees do not act outside the ambit of authority and mandate upon which licenses are issued. Other examples include specific acts that establish credit institutions or financial authorities and determine the bounds of the regulator and the supervisor.
Regulations	
Money Remittance Regulations	These regulations stipulate requirements for establishing and obtaining a license as a remittance service provider. It also provides information on the operations of RSPs and other areas including AML measures and customer protection.
National Payment Systems Regulations	These regulations usually provide for the authorization and oversight of payment service providers, the appointment of payment systems, selection of payment instruments and outline of anti-money laundering measures. These can be within the mandate of the central bank, financial authority, treasury, or ministry of finance.
National Payment Systems Sandbox Regulations	These regulations provide information on how to apply to operate a sandbox and what the documentation requirements are. It also provides information on how the central bank will consider applications, and how they will be processed, including set timelines and how they will decide whether to approve or dismiss the application.
Financial Institutions (Agent Banking) Regulations	These regulations position agent banking as a cost-effective delivery channel for offering banking services, particularly in rural areas. They also set out activities which may be carried out by an agent. Finally, these regulations provide a set of minimum standards for customer protection and risk management for agents to adhere to.
Fintech regulatory frameworks[14]	These are a structured set of rules and standards aimed at governing the activities of financial technology (fintech) entities. These frameworks incorporate requirements to mitigate risks like competition arising from diverse financial activities and aim to ensure fair market dynamics in the fintech sector.

[14] For more information on fintech regulatory frameworks, you can refer to the Financial Stability Institute's paper here.

Relevant instruments	What to be on the lookout for
Guidelines[15]	
AML/CFT/CPF Guidelines	AML/CFT/CPF guidelines set the regulatory expectations and clarity regarding AML/CFT/CPF requirements. Although a guideline document sets out some responsibilities, it is not an accountability or responsibility document that says who the policymaker is and who is the regulator.[16]
Guidelines on Agent Banking	These guidelines provide minimum standards and requirements for agent banking operations. These guidelines also position agent banking as a cost-effective delivery channel for offering banking services, particularly in rural areas.
Guidelines for e-money Issuers	These guidelines guide on the requirements for authorization to be an e-money issuer; the appointment of agents by e-money issuers and how they should operate; as well as any other related regulatory requirements. Note: where guidance on originating or terminating into an e-money or mobile money wallet is available, these should also be reviewed as they can include regulated tiering, processing and data requirements.
Guidelines for Inward Remittances	These guidelines provide the minimum requirements for providing inward (receiving) remittance services, especially when partnering with international money transfer operators (IMTO)s.
Mobile money or e-money guidelines	Mobile money/e-money guidelines address business rules governing the operation of mobile or e-money activities. It also outlines the minimum requirements or services expected from any mobile money service provider.
Other considerations	
Depending on the jurisdiction, the above legislation may need to be considered along with the relevant e-money laws, regulations as well as banking laws, foreign exchange laws and regulations. This also includes balance of payments related regulations. Always be aware that regulation cannot be interpreted nor applied outside of the scope of provisions of legislation and that guidelines can never be beyond the scope or mandate of both legislation and regulation. It is a mistake to interpret or implement any regulatory instrument in isolation.	

Once you have determined the list of relevant documents to consult, it's time to start the assessment. To reiterate: taking stock of the regulatory requirements and parameters is an important precursor to any of the innovation interventions that will be outlined in chapter 3.

Note to the reader: It's important to note that this is a high-level categorization of the compliance obligations in a jurisdiction. No regulatory regime is the same and several other instruments may need to be reviewed depending on your jurisdiction, including but not limited to public compliance communications, circulars and directives. Be sure to consider other instruments that may not have been accounted for above before proceeding to the next section.

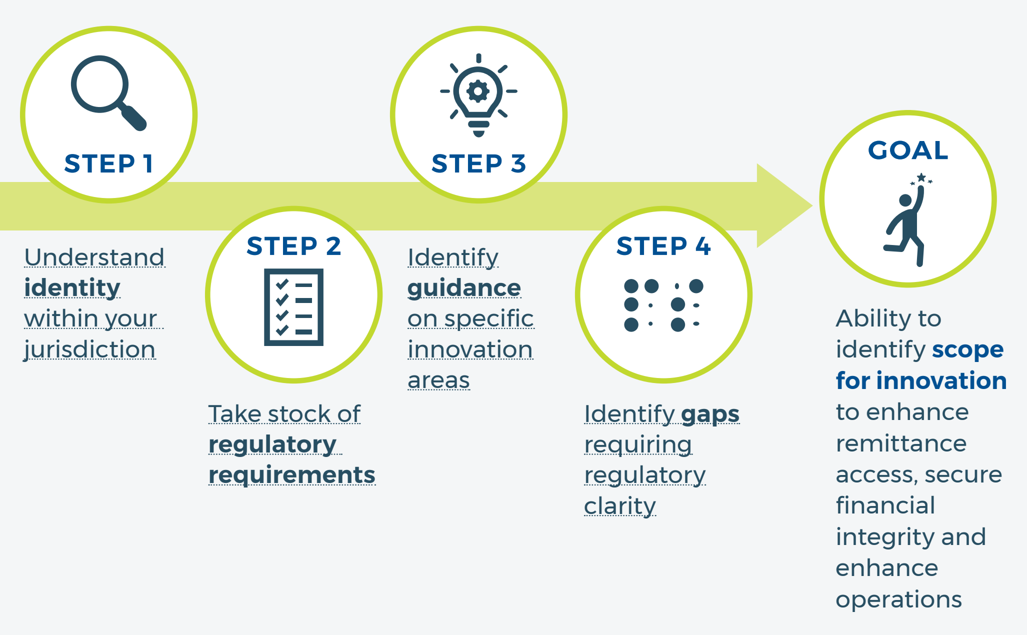
[15] Also referred to as guidance notes in some countries, e.g. South Africa. These are used to guide compliance-related activities as obligated by the AML Act. These assist with the interpretation of the Act or regulations.

[16] The fact that there is a "missing policy maker" is often one of the key challenges for AML/CFT/CPF accountability.

2.2 Guide for RSPs to conduct a regulatory assessment

Plotting the regulatory parameters within which you can innovate. Figure 1 below provides a visual overview of the key steps to take to determine the regulatory scope within which an RSP can innovate. By following these steps, you will gain clarity on (a) the KYC and CDD requirements that you must comply with; (b) what forms of identification you may accept; and (c) where there is scope for innovation in your business.

FIGURE 1: **KEY STEPS FOR AN RSP REGULATORY ASSESSMENT AS A BASIS FOR DETERMINING THE SCOPE FOR INNOVATION**


STEP 1
Understand identity within your jurisdiction
STEP 2
Take stock of regulatory requirements
STEP 3
Identify guidance on specific innovation areas
STEP 4
Identify gaps requiring regulatory clarity
GOAL
Ability to identify scope for innovation to enhance remittance access, secure financial integrity and enhance operations

STEP 1
UNDERSTAND IDENTITY WITHIN YOUR JURISDICTION

While reviewing the AML act, regulations and respective guidelines, the starting point is to look at how your country **defines identity** and then list the corresponding identifiers that you're permitted to use in the identity verification process:

- The definition of identity will most likely be contained within the national AML act or national population registry legislation of the country. The legislation, regulation, or guidance should include criteria for each class of identity, e.g. foundational identities, digital foundational identities and functional identities.
- The definition of identity will be complemented by specific examples of types of identifiers (e.g. national ID, passport, etc.), and an indication of which ones are acceptable for verifying customer identity. Specific examples or individual types of identifiers are subject to variation as new IDs are rolled out or older ones are retired.

For step 1, your specific task is to (a) determine whether the identifiers for identity verification are described or prescribed; (b) list the identifiers described/prescribed; and (c) conduct brief research to identify their value and potential limitations. In terms of (c), an identifier's value can be determined by looking at its use cases, how it can be verified (national database, biometrics, etc.), and looking at whether there are proxies for this identifier. It is important to flag the shortcomings of each, for example, whether they expire quickly, are easy to falsify, or are costly to verify.

A note on identity proxies

Some jurisdictions have identified proxy IDs, such as a mobile phone number, which can be used to verify a customer's identity. For example, in Senegal, mobile connectivity was close to 100 per cent, while identity coverage was roughly 82.7 per cent in 2021 (World Bank, n.d.; GSMA, 2021). Given that customer identification is mandated in Senegal for individuals to register for a SIM card, this means that SIM cards have potential as a proxy ID option (GSMA, 2021).

Table 4 below provides an example of how step 1 was executed in the Kenyan context under the IFAD RAI programme:

TABLE 4: **SNAPSHOT OF KENYA'S IDENTITY SYSTEM**

ID types	Issuing and governing authority	Extent of coverage	Use cases	Biometrics	Potential proxy IDs
National ID Card (NIC)	National Registration Bureau (NRB), under the Ministry of Interior	91 per cent of Kenyans above 18 years (2021)	Foundational credential which is required to access most government and financial services and a SIM card – FSPs can access database	Photo, fingerprints, signature	National ID number
Passport	Department of Immigration Services under the Ministry of Interior and Coordination of National Government	3.5 million Kenyan passport holders (2023)	Used to verify one's country of citizenship. If travelling outside of Kenya, it is used to regain entry into Kenya	Photo	Passport number
Refugee ID Card	National Registration Bureau, under the Refugee Affairs Secretariat	No data	Foundational credential which is required to access most government and financial services and a SIM card – FSPs can access database	Fingerprint, photo, signature	ID card, individual number as printed on the refugee ID card
Shortcomings identified during the Cenfri and IFAD study conducted between 2019 and 2020:[17] • As of 2019, gaps in coverage of national ID existed. As of 2018, 88 per cent of Kenyans above 18 years of age had a national ID (Caribou Digital, 2019). However, there are some left with limited access. • Long waiting times (3 years or more) for the refugee card negatively impacted remittance access for refugees and asylum seekers (UNHCR, 2020).					

Source: (NTSA, 2016; Caribou Digital, 2019; GSMA, 2020a; Kenya Immigration, 2018)

[17] This information was correct at the time the study was conducted.

Permitted identifiers may vary based on the licensing category. It's important to note that the identifiers described or prescribed can differ from business to business depending on their licensing category. For example, in Uganda, there are specific requirements for payment service providers to serve a customer with an e-money remittance. These requirements are prescriptive in nature. Table 5 below provides an overview, drawing from Uganda's regulatory framework as an example, of the different KYC requirements based on the business licence/activities:

TABLE 5: KYC REQUIREMENTS BASED ON ACCOUNT CATEGORIES IN UGANDA

Account category	Identity KYC requirements
E-money transfer transactions	For a simple mobile money transaction, customers will only need a registered phone number and a registered mobile money account.[18]
Cash-in transactions (this refers to a sender exchanging cash for an e-money remittance to be sent to the recipient, e.g. with an agent)	To send an e-money transaction by paying for it in cash, two identifiers need to be collected from customers. The first is a registered phone number and a registered mobile money account. The second is an "acceptable passport photo" and identification card (also referred to as a photo-bearing ID like a national ID card) (BOU, 2021).
Cash-out transactions (this refers to a receiver exchanging an e-money remittance for cash, e.g. at a bank)	When receiving an e-money remittance and exchanging it for cash, an "acceptable passport photo" and a national identification card (also referred to as a photo-bearing ID) are needed. Foreign nationals are allowed to use a passport or refugee identification as acceptable identifiers.
Note: the KYC requirements are the same for individuals who are allowed to transact with higher limits.	

Source: Adapted from Bank of Uganda (2021).

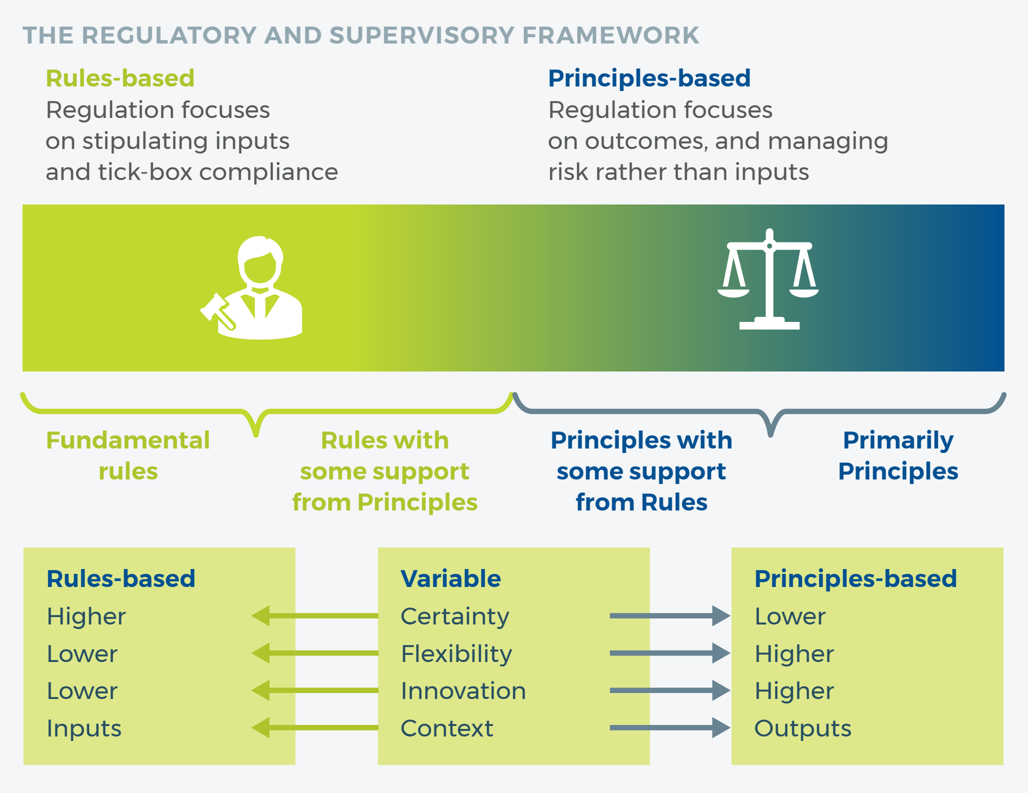
Important flag for step 1: how the national transition to a principles- and risk-based approach impacts RSPs. In going through the process to determine identity requirements and proxies in your jurisdiction, it is important to understand whether the regulator applies a first principles and outcomes-based proportionate approach, a defined risk-based approach, a rules-based compliance approach, or some variation along that continuum. This will dictate how the regulator defines identity, which identifiers can be used and what the requirements for identity verification are. International best practice, as outlined by the FATF, mandates following a risk-based principles approach to KYC and CDD as opposed to a rules-based approach or outcomes-based approach.[19] However, in practice, very few (if any) regulators practice a purely principles risk-based approach. Most operate on a spectrum between these two. The diagram below explains the spectrum of approaches and how key variables such as certainty, flexibility, innovation and the role of context vary along the spectrum.

[18] In many countries, a mobile number is being employed as an effective proxy ID.

[19] A rules-based approach can be based on many risk factors beyond mere compliance, for instance a higher risk geography could be de-risked by rule with very little to do with compliance.

The ideal approach, based on the FATF's guidance, is to move from a purely rules-based towards a principles risk-based and outcomes-driven approach to regulation.[20] This means that instead of creating rules that must be applied regardless of risk, the regulator requires you to apply a process where risk controls should be implemented based on the identified risks and clear potential outcomes rather than just inputs.

FIGURE 2: **THE SPECTRUM OF APPROACHES TO KYC AND CDD REGULATION**



THE REGULATORY AND SUPERVISORY FRAMEWORK

Rules-based
Regulation focuses on stipulating inputs and tick-box compliance

Principles-based
Regulation focuses on outcomes, and managing risk rather than inputs

Fundamental rules

Rules with some support from Principles

Principles with some support from Rules

Primarily Principles

Rules-based		Variable		Principles-based
Higher	←	Certainty	→	Lower
Lower	←	Flexibility	→	Higher
Lower	←	Innovation	→	Higher
Inputs	←	Context	→	Outputs

Note: The **risk-based approach**, as mandated by the FATF falls along this spectrum

[20] In contrast, a compliance focussed rules-based approach fixates on compliance inputs by rule.

The diagram above illustrates a few of the distinguishing features between the rules-based and principles-based approaches. These distinguishing features are included below:

- **Certainty.** The rules-based approach is highly certain in the sense that institutions know what the regulators expect and vice versa. They also know what they can be fined for as requirements are mostly based on a "tick box" approach. For example, if the requirement is to have proof of address documents, then those who are non-compliant know that it creates the liability for fines. On the other hand, the principles-based approach requires constant engagement between regulators and institutions and is therefore not just a point-in-time engagement.
- **Flexibility.** The rules-based approach is not flexible, as RSPs either meet information requirements or risk getting fined. On the other hand, the principles approach is flexible and only requires institutions to justify to the regulators and board the various measures they put in place.
- **Innovation.** The rules-based approach does not promote innovation as it is focused on set requirements. For example, if it requires institutions to have proof of address as part of their due diligence, it will not override it for biometrics or a similar more robust innovation. On the other hand, the principles approach is open to this and focuses more on whether whatever measure is in place achieves the stated AML/CFT outcomes.
- **Context.** The rules-based approach emphasizes inputs (i.e. what is required to comply e.g., documents) while the principles approach emphasizes outputs and outcomes (i.e. the ML, TF and PF risks being mitigated). Finally, under the rules-based approach, the interaction between RSPs and regulators is restricted to assessment periods, while under the principles approach, the engagement is continuous.

To identify where your country lies on the spectrum, we recommend you review your anti-money laundering act, regulations and respective guidelines. If identity verification is outcome-focussed in nature (in other words, it does not specify the identifiers but leaves you with the flexibility to demonstrate that whichever identifiers you are using addresses money laundering, terrorism financing and proliferation financing risks modalities in line with the FATF framework) then your regulations are likely closer to the principles-based outcomes-focused approach as they seek effective risk mitigation outcomes instead of near perfect input documents for compliance audits with limited effectiveness. However, if your identity verification regulations are prescriptive (they tell you what you *must* do and which identifiers to use), then your regulations are likely closer to the rules-based approach part of the spectrum. Table 6 below provides further information on what each approach may mean for an RSP:

TABLE 6: OVERVIEW OF THE RULES-BASED AND PRINCIPLES-BASED APPROACHES

Rules-based approach	Principles risk-based approach
What this means for you	
As an RSP, this means that you must use the prescribed identifiers and processes to verify a person's identity,[21] thus translating into less flexibility around simplifying KYC and CDD measures. Despite rules-based prescribed processes for undertaking KYC, there are still potential innovations that can be leveraged for more risk-effective and inclusive outcomes. This includes using digital forms of proof of address, e.g. if your AML/CFT laws state that proof of address can be established by "any other means", or even applying simplified CDD measures for specific for-purpose remittance products were allowed in the AML/CFT laws. Particularly where the compliance effort in respect to low or perceived risks distracts focus and resources from mitigating proven higher risk elements.	As an RSP, this means that you have more flexibility to apply tools that enable financial inclusion, however, there's an increased onus on you to ensure that these are accompanied by effective and appropriate risk mitigation measures. RSPs will likely be permitted to leverage key areas of innovation such as simplified KYC and CDD, remote onboarding, and identity proofing enabling more concentrated focus on empirically assessed high or higher risks and vulnerabilities aligned to everchanging modalities. Some countries would have developed guidelines for financial institutions on how to leverage these areas of innovation, where this is not available, the FATFs guidance can be used. For example, the FATF's guidance on identity proofing.

As outlined above, most regulators are still transitioning to a risk-based and outcomes-focused approach. This often means that while the approach to identity *on paper* may be transitioning towards being more principles-based, *in practice* some remaining rules-based practices may prevent full implementation of these principles. Therefore, it's always important to pick up on any caveats that go with the identity verification process as a final checkpoint in understanding identity in your context. In practice, it may be inevitable to undertake ineffective or disproportionate mandatory compliance practices but still effectively mitigate empirically assessed material risks without materially impacting product viability. Open dialogue with the regulator, directly, via an industry body or academia on needless or disproportionate compliance is an important feedback loop that can benefit the overall effectiveness and viability of the industry, sector and country. The box below provides an example, drawing on the case of South Africa.

[21] Note that a rules-based approach can introduce more risk if institutions rely heavily on a rule and where the identifier can be flawed or not easily verifiable. For example, outlining the voter's card as an identifier for financial services, where it is easily falsified in some countries or corruptly issued. This approach can therefore work only if there are appropriate mitigations like an advanced and accurate digital ID verification system in place to mitigate risk.

BOX 1: Transitioning to a principles risk-based approach – the case of South Africa[22]

Since 2017, South Africa has made significant strides towards principles risk-based approach and moved away from prescribing identifiers and verification processes.

Chapter 2 of Guidance Note 7 speaks to Customer Due Diligence Measures[23] (Financial Intelligence Centre, 2017). Section 83 of chapter 2 states that financial institutions must first obtain a range of information about a client and then verify that information by comparing it to information found in "documents or electronic data issued or created by reliable and independent third-party sources" (Financial Intelligence Centre, 2017). Section 83 goes on to detail that "the nature and extent of verification of clients' identities must be determined taking the assessed ML/TF risks associated with the relevant business relationship or single transaction into account" (Financial Intelligence Centre, 2017). Despite the clearly promoted flexibility, Guidance Note 7 recommends that financial institutions "should, as far as is practical", use government-issued or controlled sources as the means of verification when verifying basic identity attributes (Financial Intelligence Centre, 2017; Cenfri & IFAD, 2023).

Despite the above, there are some instances where remittances may be subject to additional regulations which could either support or contradict the regulatory approach to verifying identity. For example, in South Africa, all remittances must comply with the Exchange Control regulations, which are rules-based in nature as they prescribe the identifiers that financial institutions must use per customer category for KYC and CDD (Cenfri & IFAD, 2023).[24] Therefore, it is vital to consider other regulations that exist which could have a bearing on KYC and CDD requirements.[25] This experience shows that, since many regulations are connected, even implicitly, it is not enough to merely add risk-based approach terminology in the regulations. Instead, enabling legislation and its implementation needs to be outcomes-focused and take a holistic view of regulations that could be affected by the intended changes.

[22] Although currently grey-listed due to other AML/CFT weaknesses, this guidance from countries like South Africa is aligned with the FATF's recommendations. The assessment of Financial Intelligence Capacity and ability to guide to the market was assessed quite favourably in South Africa's most recent Mutual Evaluation. Despite this positive assessment, implementation of the guidance by industry may often be slower requiring active and regular engagement to narrow the gap.

[23] For more on Guidance Note 7, read here

[24] Therefore, it is essential to view the regulatory approach considering regulations that apply to a specific licensing category and with a different purpose, to prove residency for foreign exchange allowances as opposed to CDD. De-conflating the purpose of the documents allows for more proportionate measures.

[25] This includes regulation under another authority, e.g. the Post Office or the communication authority which manages mobile money requirements. In practice this means that money transfer operators sending money within the country can leverage the flexibility of the principles-based approach – they have a descriptive system. However, remittance operators, sending or receiving money from outside of the country, may not yet do so as they have a prescriptive system.

STEP 2
TAKE STOCK OF THE REGULATORY PARAMETERS FOR YOUR RSP

After establishing how identity is defined in your jurisdiction, and which identifiers you may use for identity verification, the next step is to take stock of the complementing regulations that apply specifically to your licensing category. These often determine how you must keep customer records, what kind of products and services you may offer and to whom you may offer these. Table 7 below provides key areas to look for when considering specific regulatory parameters:

TABLE 7: **KEY AREAS TO CONSIDER WHEN REVIEWING REGULATORY PARAMETERS**

Parameter	What to look for
Record storage requirements	• Do documents need to be stored physically or may they be stored digitally? • Where must records be stored? • For how long must records be stored? • For what purpose may the stored records be used? • What are the regulatory limits of use of stored records? • What are the consumer consent considerations in each application?
Tiered transactions	• Certain KYC and CDD requirements can be decreased or waived for transactions below a certain amount • Search for sections in the regulation that indicate whether CDD should be carried out before establishing and during normal business operations with a client
Third party requirements	• Are you allowed to use a third-party to conduct CDD and KYC on your behalf for your, or your partners' remittance products?
Additional processes for vulnerable groups, such as refugees.	• KYC and CDD requirements are often challenging for vulnerable groups, like refugees. Are there any extra KYC and CDD requirements for certain groups of people, e.g. vulnerable people, as per your regulations?

In your review, also take proactive note of upcoming changes to regulation or other relevant rules. When it comes to reviewing your regulatory framework, it is best to be proactive instead of reactive. This means that you need to keep a watchful eye on any upcoming regulatory changes and the publication of guidance or notices, such as the introduction of a new national ID, new guidance notes on areas of innovation or new supervisory guidelines on the implementation of new requirements. This can be done by proactive ad hoc consultations and engagement with financial sector regulators and supervisors, through leveraging and attending existing platforms and engagements between institutions and regulators and setting internet alerts to notify you of upcoming changes. Another dimension, especially for subsidiaries of institutions headquartered in regional hubs (such as Ghana, Kenya, South Africa, or Nigeria) is to keep an eye on regulatory changes in the hub country. This is because changes made by a head office in the hub country will likely impact the subsidiary institutions in the spoke country. Also important to keep track of institutional changes in policies and procedures, especially at the head office level and implications for local-level policies and procedures. These must be further aligned with local regulations and guidance.

Reflection point

Steps 1 – 2 have explored and informed the scope for innovation based on existing regulatory frameworks. After these steps you should know:

- The identifiers available to be leveraged for identity verification, and which you may use based on your licencing category
- The complementing regulations that you must stay compliant with.

To refer to the sports analogy, these two steps have highlighted the field and the rules of the game. Once you know where and how to play, you can look at how to innovate to enhance remittance access and improve your competitive edge. That is considered in the next two steps below.

STEP 3
IDENTIFY GUIDANCE ON SPECIFIC INNOVATION AREAS

Once the regulatory parameters have been drawn up it becomes possible to develop or adopt existing innovative interventions to enhance your business while complying with the jurisdiction's regulations. This could entail introducing mechanisms to digitize manual processes, such as record keeping, or even introducing a tiered product for lower-risk customers. To start your innovation journey, it is important to first take stock of the innovation that may already be encouraged in your jurisdiction. Some regulators have encouraged or supported innovation within their jurisdictions by (1) guiding how to implement certain innovations, (2) explicitly permitting certain innovations, or (3) creating platforms to encourage innovation, e.g. sandboxes. Table 8 below provides some examples from the IFAD PRIME countries of how some regulators have done so:

TABLE 8: COUNTRY EXAMPLES OF INNOVATIVE INTERVENTIONS

Type of innovation	Regulatory premise/guidance	Example from IFAD PRIME countries[26]
Remote onboarding	Non-face-to-face onboarding is typically discussed in the AML/CFT Act or Guidelines on AML/CFT. This means that institutions can verify customer identity without seeing them in person. Remote or digital onboarding can be of equal or lower risk than face-to-face onboarding due to the potential for cross-validation between multiple digital points and less reliance on manual processes.	In Uganda, regulation allows for remote identity proofing, collaborative digital KYC systems for verification and flexible requirements for FDPs. E.g., a digital ID.
Alternative Identifiers	AML/CFT Acts can allow for identifiers other than the national ID to be used to access remittances. For example, biometrics can provide a robust form of functional digital identity, that may have legal effect under proportionate regulatory frameworks. This could also remove the need for paper-based identifiers, especially if the identifier can be verified online and verified against a digital foundational ID e.g. the Ghana Card.	In Ghana, although the Ghana Card is mandated, for customers who do not have an identity document, the AML/CFT Guidelines allow for a person accompanying the customer to present a letter or statement as proof of a customer's identity along with their valid Ghana card. Outside of the PRIME countries, the Bank Verification Number (BVN) in Nigeria is a good example of a biometric-based functional digital ID specifically for the financial sector.
Identity proofing	Identity proofing refers to the process by which an identity service provider collects, validates and verifies information about a person and ends up with one unique individual within a population (FATF, 2020). Determining whether the regulation allows for this, will establish whether you can use ID proxies and digital IDs.	In South Africa, Section 89 of Guidance Note 7 makes clear provisions for identity proofing as it states that "*Corroboration of a person's identity … can be in documentary or electronic form. Moreover, many of a person's identity attributes accumulate over time and can be found in the person's so-called "electronic footprint"* (FIC, 2017). The FIC encourages the use of information in electronic form to corroborate a prospective client's information against multiple third-party data sources".
Regulatory sandbox	Sandboxes allow RSPs to develop new services, products or solutions that are not yet covered under existing regulation.	Ghana has launched a regulatory and innovation sandbox for financial sector innovators.[27] The Bank of Ghana's regulatory sandbox framework outlines the documents needed and requirements for RSPs to enter the sandbox.
Customer profiles	Customer profiles enable customer transaction behaviour tracking to better manage risk. Through flexible recordkeeping requirements, regulators can remove the need to repeatedly present IDs and instead capture customer details on a profile.	In Kenya, the Integrated Population Registration Services (IPRS) data base can result in the physical ID only being required for the first transaction. Thereafter, only the ID number will be required, with other information automatically accessed and filled out.

Source: Cenfri & IFAD (2023)

[26] These examples are based on the countries where these innovations are most pronounced and have taken effect. Countries that are still working towards or planning to do the same have not been included. PRIME refers to the Platform for Remittances, Investment and Migrants' Entrepreneurship. The seven countries referred to are The Gambia, Ghana, Kenya, Morocco, Senegal, South Africa, and Uganda.

[27] The Bank of Ghana stipulates preference will be given to products and services "leveraging blockchain technology, remittance products, crowdfunding products and services, e-KYC platforms, regulatory technology (RegTech), supervisory technology (SupTech) digital banking, products and services targeting women financial inclusion" (Bank of Ghana, 2021).

Remember to review additional supporting regulations and/or guidance papers depending on the area of innovation you are interested in. After you have reviewed all the relevant regulations and legislation there may still be other regulations that may be of relevance, for example, data and customer protection frameworks. After taking stock of these, you can also consult updated FATF guidance, like the FATF's guidance on digital identity, which can provide a better picture of potential innovations. In the event the innovation you are aiming to introduce is fundamentally new in your jurisdiction, this robust regulatory research and backing will place you in a strong position to approach the regulator and request access to innovative platforms, such as sandboxes, where you can effectively test your innovation in a market-like environment. If a sandbox is in place, the feedback and learnings from the sandbox experience should then be shared with your regulator to spur further innovation in your market (See the Regulation for Innovation Toolkit for more). experience should then be shared with your regulator to spur further innovation in your market.

STEP 4
IDENTIFY GAPS OR CONTRADICTIONS REQUIRING REGULATORY CLARITY

After completing all the steps, you may still have questions requiring regulatory clarity or support, particularly where there are seemingly gaps or contradictions in definitions and/or regulations. There are two mutually reinforcing ways to address this. These involve consulting the regulator (directly for clarity) and/or consulting the FATF's frequently updated guidance, as well as guidance from the European Union (EU) directives or guidance from the European Commission, the Financial Stability Board, or the European Central Bank for clarity. It is advised to see these methods as a two-pronged approach, as consulting the regulator could be beneficial for understanding the broad regulatory requirements in your country while expanding your search to look at international best practices and guidance will fill any gaps about the latest changes and updates to best practices. Given the different levels of maturity across jurisdictions on these issues, it's always best to ensure that whatever guidance from FATF and other related bodies is in line with local regulatory expectations.

Reflection point

Steps 3–4 have focused on identifying areas of innovation and on the potential scope for innovation provided by guidance, or limitations to those areas for innovation for which further clarity is needed. After these steps you should know:

- Which areas of innovation are permitted and encouraged in your jurisdictions
- Which complementary regulations you may need to apply to certain innovations
- How to address lack of regulatory clarity

Waypoint for RSP readers

Chapter 2 has prepared you to develop a comprehensive regulatory analysis suited to your institution.

The **next step** is to identify areas for innovation to enhance your remittance business. With this knowledge you will be able to develop or select an innovative intervention to enhance remittance access/enhance your remittance business within the regulatory framework. **This will be covered in chapter 3 below.**

3

Implementing remittance access innovations

This section provides a step-by-step guide on how an RSP can implement innovative interventions to address KYC and CDD barriers. This section provides a guide for how to implement select interventions which correlate with the challenges explored in chapter 1. The contents draw on the implementation plans of five innovative interventions implemented under the RAI programme. These interventions are:

- Conducting a risk assessment and developing a proportionate response
- Building a digital ID database
- Drawing up remittance customer profiles
- Replacing manual forms with printed receipts
- Implementing a model for agent expansion and management

Guide: How to read this chapter

Each intervention starts with a **checkpoint**. This checkpoint will provide you with more information on the intervention, specifically what it's about, what its key benefits are and what resources you may need (considering time, capacity, etc.) to implement this intervention. This section should allow you to (a) align your internal expectations and (b) gather the appropriate resources before you start planning and implementing the intervention.

The checkpoint is followed by a **step-by-step implementation guide**. We recommend you first read through all the steps, then consider what they would look like in your organizational context – who would take responsibility for what, how much time this would take – and then you start implementation.

The implementation guide is followed by **key lessons** regarding this intervention. These lessons have been captured from non-confidential learnings with other institutions that have implemented this intervention along with lessons from the Cenfri implementation teams. Consider these lessons when you do your intervention planning – leverage them to build in relevant contingencies and additional steps that you may need to take.

Finally, each intervention is concluded with guidance on how to **measure the success or impact** of the intervention.[28] Measuring impact is not something that just happens at the end, the data needs to be generated and tracked from the get-go, thus it is very important to formulate a plan for impact measurement right from the start.

3.1 Risk assessment and proportionate response

FATF recommendation 1 mandates institutions and jurisdictions to identify, assess and understand the risks that they face related to money laundering, terrorist financing and proliferation financing and take action to mitigate the risks. The risk-based approach requires responses and actions taken by institutions and countries to be in line with and proportionate to the risks they face.[29] A risk assessment is therefore key to any organization's overall AML/CFT programme, strategy as well as engagements with regulators.

INTERVENTION CHECKPOINT

Disentangling risk and discovering opportunities for innovation by conducting a thorough risk assessment. All institutions are exposed to a multitude of risks which affect their business functions. This includes fraud risk, money laundering risk and compliance risks. However, these risks are often not well understood or, in many cases, are conflated with one another. As a result, institutions often have poor, inadequate or inappropriate risk control or mitigation measures in place. Subsequently, RSPs may not have a clear picture of the types of risks facing their business or a reliable quantification of the degree of exposure and magnitude of the potential impact of those risks. This limited understanding of risks inhibits innovation. To address this, institutions

[28] If you wish to conduct a cost-benefit analysis of each intervention, you can refer to Cenfri's previous work on the elements that affect compliance cost, linked here.

[29] Proportionality also relates to the institutional and country contexts as well as the key risk factors such as customer, product, geography, and delivery channel. For example, a customer base that transacts very low amounts of money periodically and consists mostly of low income or rural people cannot be inherently high risk.

should perform a holistic and thorough risk assessment to identify the different types of risks, how each impacts business and to test the effectiveness of risk mitigation measures. This should also be aligned to the size of the business, organizational complexity and the viability plus addressable markets of the remittance product(s).

The risk assessment and proportionate response intervention is both a standalone and precursor intervention. The risk assessment can be a standalone intervention, as discussed above and as explored in this section.[30] However, it is also a precursor intervention to identify other opportunities for innovation such as risk rating agents as well as the basis for simplified due diligence for less risky customers. For example, a risk assessment and proportionate response intervention can reveal that the majority of over-the-counter (OTC) customers are low-risk and are sending or receiving low-value amounts. This highlights the opportunity to develop and introduce simplified KYC accounts that require less documentation, thereby helping to enhance remittance access and financial inclusion.

The fallacy of “zero tolerance” to ML-TF risk. Money Laundering and Terrorism Financing risk will always be present in business dealings. There can be a question about the extent of risk, but risk cannot be eliminated. So “zero tolerance” to risk is a fallacy as it can only be achieved where there is no business activity. Rather than reassuring and confirming that ML and TF risks are well managed, such an approach signals the following: (1) the RSP is applying a blanket approach to risk and not considering the likelihood and severity of each risk; and (2) the RSP is likely applying a tick-box approach to managing risk. The risk assessment and proportionate response intervention is thus also an opportunity to rethink your approach to risk and to strengthen your alignment with the principles-based approach discussed in chapter 2.

Set your objectives. Before you enter the risk assessment intervention, you need to be clear on what your objectives are. Table 9 below indicates how the risk assessment intervention can meet your specific objectives. Important: These objectives are interrelated and not mutually exclusive:

[30] Note: the risk assessment provided for in this toolkit is a business risk assessment. There are several varieties of risk assessments, including sectoral or more granular risk assessments. There are also different ways of conducting risk assessments. The approach that has been used in this toolkit is a simple but effective methodology that can be geared up to be more dynamic when the organisation’s systems, processes and people allow for this.

TABLE 9: USING THE RISK ASSESSMENT AND PROPORTIONATE RESPONSE INTERVENTION TO MEET YOUR OBJECTIVES

The risk assessment and proportionate response intervention can meet two main objectives	
If your objective is to:	**The risk assessment and proportionate response intervention can help you reach these objectives by:**
1. Mitigate ML, TF, PF risks and apply risk-based approach as per FATF requirements. Strengthen your organization's risk assessment	Strengthen your organization's risk assessment by: • Understanding the ML, TF, PF risks and applying a risk based/ proportionate approach • Setting and defining your institution's risk appetite based on understanding of above risks • Developing controls that are proportionate and mitigate risks faced • Applying compliance resources more appropriately and to improve the competitiveness of products, not only in terms of access barriers but in relation to costs and revenue. Essentially, this will enable you to manage compliance cost appropriately and redesign products with wider addressable markets and lower cost to income ratios through targeted product development, i.e. designed for low-risk low compliance costs and key lower risk target markets. This is in reaction to the valid comment about the business motivation
2. Enhance remittance access and serve more customers	• Use data to re-rate customers (including low income and rural) based on actual ML, TF, PF risk posed • Understanding and evidencing the risks facing your business, specifically risks associated with entering new partnerships, channels or adjusting your product offering • Reaching new target markets (including vulnerable and excluded groups such as poorer, low-risk segments) more effectively • Opening new remittance channels or corridors • Expanding your product offering

The cornerstone of a risk assessment is to (1) include a variety of risk factors in the risk assessment and (2) insert accurate and up-to-date transaction and customer data. This will allow you to design your risk mitigation measures such as customer identity verification, transaction monitoring, sanction list screening and product and channel risk assessment in a way that reflects the actual risk exposure of your business.

Before you jump in, weigh up the costs and benefits. To determine whether this intervention is worthwhile, it is important to compare the costs and benefits associated with implementing the intervention. The table below provides a guide for how you can think about estimating the costs and benefits of the intervention within your context. There are two scenarios for this intervention, one being an RSP merely updating their existing risk assessment framework to make it more proportionate, and the other being where an RSP does not have a risk assessment and proportionate response framework and will be starting from scratch. Costs associated with the latter are indicated below.

TABLE 10: COSTS AND BENEFITS ASSOCIATED WITH IMPLEMENTING THE INTERVENTION

Benefits
Comprehensive, validated and up to standard proportionate risk matrix that can provide a tailored and accurate view of your business risk factors and profiles considering emerging risks and global trends. Thereby enhancing your ability to mitigate and address risk if and when they manifest. **Reduced risk of fines.** Participating RSPs under the RAI found that redirecting their efforts to high-risk customers through more effective risk rating helps in their compliance efforts. This frees up compliance resources and helps to reduce the risk of fines. **Fewer excluded customers.** Customers that have been re-rated are no longer at risk of being excluded. Under the RAI programme participating RSPs found that, by improving their risk assessment and proportionate response system, all barriers related to unnecessary documentation requirements were removed, thereby benefiting thousands of customers per month. It also helped to reduce the number of false positives, so that more customers can be served who were previously falsely flagged by the sanction screening process. **Increased customer base.** By risk rating and relying on their third party's due diligence measures, participating RAI RSPs could onboard numerous new customers. With a more accurate risk rating in place, new remittance corridors could also be opened, which resulted in additional new customers each month, resulting in a substantial increase in the overall customer base.
Costs
Dedicated **time and capacity**, for approximately 6–8 months to upgrade, enhance and improve the risk matrix to align with international best practice. This is specifically applicable to the compliance team. **Data related costs.** This will depend on the state of your data capturing, storing and analysing capabilities. If these are outdated, there may be costs associated with training your team, hiring an expert, or investing in a digital solution to support the retrieval, curation and analysis of data. **Cost of maintenance and upkeep.** The risk assessment matrix will need to be kept up to date, as this is a continuous process, and not a once-off solution. Therefore, depending on the state and capabilities of your compliance team, there may be cost associated with continuously training your team, or retaining an expert/digital solution to support retrieving, curating and analysing data in the long term.

Getting ready – key considerations when implementing this intervention

- **Time:** depending on where you are in this process (updating/enhancing or starting afresh), you should allow between approximately six months (without delays) and an average of eight months (with moderate delays) from design to implementation. This is estimated based on the assumption that you will have managerial buy-in, required capacity and minimal approval or technical delays.
- **Capacity:** a project champion who will manage the implementation and coordinate with key stakeholders such as regulators (where needed), IT and technology experts and data analysts who can incorporate data into the risk assessment.[31] The best-case capacity scenario is having a compliance officer or team with the requisite AML/CFT, IT and data analysis skills in house. Where this is not possible, it can be outsourced in line with the organization's policies and procedures.
- **Key dependencies:** AML/CFT/CPF risk and internal or external capacity to conduct data analysis. Where an AML/CFT audit has been undertaken, findings relating to overall risk environment and risk assessment should be considered.
- **Regulatory considerations:** consider the regulatory assessment for your country, specifically drawing on AML/CFT acts, regulations and guidelines. Key things to consider include documentation requirements that would feed into risk assessment, when it should be conducted (e.g. before or after the business relationship is established) and how often it should be conducted (e.g. once-off or throughout the course of the relationship). Also consider any regulatory findings and feedback regarding risk assessment.

[31] A compliance officer or related staff member could undertake a preliminary manual exercise in assessing and analysing the data and applying it to a risk assessment model. Such an exercise would provide preliminary insights into their risk mitigation and would be invaluable in scoping a more comprehensive or targeted approach at systematising risk assessments.

What success can look like – testimonial from the RAI

Amal Express Money Transfer (Amal Express) implemented the risk assessment and proportionate response intervention. They have shared the following feedback regarding the intervention:

- "This [intervention] **assisted us in lowering risks** [and KYC and CDD requirements] for clients who were receiving small amounts of money from relatives who are in high-risk jurisdictions."
- "[In turn] this helped us **reduce the amount of time** [to serve a customer] and made the **customer feel less harassed**, especially women who were receiving funds for family support".

Amal Express is a cross-border business payments provider and is transforming how businesses can expand globally through a diverse payment network. In 2016, they completed over 100,000 transactions for their consumer and business clients. They continue to innovate, developing new ways to send money through digital, mobile, and retail channels, with an array of convenient pay-out options to meet business and consumer needs.

A STEP-BY-STEP GUIDE TO IMPLEMENTATION

Summary

Conducting a risk assessment entails the following six steps, each of which is explored in this sub-section:

- Step 1: Identifying the inherent risks and the key drivers of these risks
- Step 2: Updating your risk appetite
- Step 3: Setting up a risk assessment and proportionate response framework and importing data to it
- Step 4: Using the updated risk assessment matrix to enhance your business
- Step 5: Developing an action plan to implement changes from the risk assessment
- Step 6: Empowering staff for implementation

It should be noted that where a compliance audit and regulatory examination has been done, the starting point is to review the findings in relation to the highlighted gaps and shortcomings of the overall AML/CFT programme as well as risk assessment.

Step 1: Identify the inherent risks and the key drivers of these risks. This step, the point of departure for conducting a risk assessment, entails building a good understanding of the risks involved in the remittance business. These are introduced in Table 11 below. Firstly, define your **risk types**. This includes ML risk, TF risk, PF risk, compliance risks, exclusion risk, illicit flows risk and trade-based money laundering risk.[32] As discussed in the checkpoint above, the types of risks are often conflated, resulting in an overfocus on compliance risk. Subsequently, institutions often expend energies on controls that mitigate compliance risk mistaking it for ML, TF and PF risk controls. This often places the organization at ML, TF and PF risk and can lead to negative regulatory and mutual evaluation feedback. The second part of the first step is to consider the

[32] Refer to Table 27 in Deep dive 3: A guide for regulators to assess regulations against inclusive integrity goals and best practice for the definitions of these risk types.

impact of the different **risk factors** for each different risk type. For example, the following factors should be considered when assessing risk:

- Product
- Delivery channel
- Geographical factors
- Client
- Agent network
- Other relevant contextual factors as defined per jurisdiction[33]

Next, you combine the key risk types with the risk factors to understand how they manifest in a particular jurisdiction. The key focus here is to de-conflate different types of risks. The box below discusses how to know which risk type to focus on, while Table 11 below provides a non-exhaustive list of the risk factors that should be evaluated by each risk type, as well as example risk factor attributes.

BOX 2: How to know which risk types, factors and attributes to focus on

Table 11 below showcases risk types, factors and attributes. In the context of this toolkit, which focuses on inclusive financial integrity, **a risk type** is defined as the broad category of financial integrity risk, such as money laundering or terrorist financing. Risk types also present the initial characterization of the risks an organization is exposed to (Open Risk Manual, 2019). **Risk factors** go one step further and represent various ways within which an activity or product can pose a risk for each risk type. Finally, the list of attributes represents specific characteristics of risks that can be measured (Risk Publishing, 2023).

Not all the risk types and factors in table 11 below necessarily apply to your business, nor are all relevant based on your objective. The risk types and factors you assess will depend on (1) what you want to achieve through the risk assessment – what your **objective** is in doing a risk assessment and (2) your business strategy (that is, your ideal outcome). For example, if your objective is to enhance remittance access by introducing tiered accounts, or simplified accounts, for low-risk customers, then you must first assess the risk posed by all your customers to identify what portion fall into the low-risk category. Note that these customer risks should be assessed in respect to other customer attributes, geography, which indicates whether a customer is in a high-risk area or not, as they are often linked. Based on this you will be able to leverage the information for data-based decision-making on (a) whether a simplified account is in demand among your customer base; (b) whether it could offer value to your customer base; and (c) how to mitigate the risks arising from such a venture. However, if your objective is to open new corridors, then you need to assess your geography risk to assess the viability of the channel.

[33] For example, technology, regulatory and governance, partnerships, control effectiveness, compliance, and so forth. It will also be important to assess the impact of your contextual realities including regulatory and governance-based nuances.

TABLE 11: RISK TYPES, FACTORS AND ATTRIBUTES[34]

Risk types (example)[35]	Relevant risk attributes examples based on risk factors (Product, Channel, Customer, Geography)
Money laundering risk	• Product allows for medium to large value flows • Technology allows for rapid transactions • The regulation prohibits sender/receiver tracking • Poor partner due diligence
Terrorist financing risk	• Product open to high-risk jurisdictions • Transaction purpose obscured or unclear • Limited counterparty information • Limited third-party due diligence • Client linked to NPOs • Limited and infrequent sanctions screening
Proliferation financing risk	• Links to high-risk jurisdictions • Product geared for large values with limited documentation • Limited trade logistics or trade finance tracking • Client linked to or approximate to high-risk industries or resources • Limited and infrequent sanctions screening
Exclusion risk	• Mandatory due diligence checks across all risk types and all risk attributes • Limited delivery channels due to perceived risk • High barriers to entry for agent network • Mandatory input documents by regulation • Limited partnerships or disproportionate third-party partnership due diligence • Limited technology channels or instruments • Domestic only or high restrictions on external jurisdictions • Not served due to geography (for example not servicing specific areas due to perceived or real risk of criminality, etc.)
Illicit flows risk	• Exposure to high-risk countries for the IFFs according to the National Risk Assessment (NRA) • Product supports medium to high value inflows with no or limited reciprocal trade documentation • Clients linked to high-risk resource areas, processing, or trading • Limited partner TPDD • Regulatory requirements limit access to transaction tracing • Limited to no monitoring or tracing of trade finance and trade logistics

[34] Note: for this toolkit, this is a simplistic representation of the risk types, -factors and -examples, as the risk factors and attributes interlink

[35] The ML, TF, and PF risks are key risks defined by the FATF and the focus of AML/CFT programs at the country and institutional level. Financial exclusion risk, illicit financial flows risk and Trade-based money laundering risks are key risks impacting the AML/CFT program for an institution or country and linked to the above ML, TF, and PF risks. Illicit financial flows risk and trade-based money laundering risks are part of predicate offences that underlie ML, TF, and PF risks. Financial exclusion risk has been officially recognized by FATF as a key risk to financial integrity and key aspect of inclusive integrity. Excluding significant portions of the population and transactions from the formal system creates a parallel informal system that can be taken advantage of by money launderers and criminals.

Risk types (example)[35]	Relevant risk attributes examples based on risk factors (Product, Channel, Customer, Geography)
TBML (Trade-based money-laundering risk)	• Historical links with free trade zones or country products only trace back to free trade or freight staging jurisdictions • Limited trade logistics documentation required • Client payments incoming or outgoing not closely linked with trade logistics • Client linked to trade, logistics or resource sectors. • Limited due diligence by partner or correspondents. • High number of services or transactions not linked with specific trade contracts • Limited or no tracking and tracing and repatriation of trade proceeds by authorities • No legal obligation to report trade proceeds

Finally, end off step one by identifying the drivers, or causes, of these risks individually and collectively, however, they manifest, from empirical evidence.

Step 2: Update your risk appetite. An organization's risk appetite refers to the level of risk, per identified risk, that is regarded as acceptable or tolerable in pursuit of a business's objectives (ACAMS, 2022). It is normally captured as a high-level statement that then informs all business activities and processes.[36] The risk appetite should also correspond to, and align with, the controls that a business has in place. As discussed above, having a zero-tolerance approach to ML, TF, or PF risks is inconsistent with FATF's risk-based approach and business. The risk-based approach implies that more resources should be allocated to areas where risks are higher. Having controls in place for addressing risk entails acknowledging that the available controls can reduce the exposure to specific elements of the risk, but never eliminate it. Therefore, setting a risk appetite is key in setting the tone and informing controls and the overall approach to risk management. Setting your risk appetite requires a good understanding of the overall risk that your business is exposed to, based on empirical data and detailed analyses. On this basis, a view of the risk appetite in the context of the specific entity can then be made. In this step, you will need to review your risk appetite statement and update it based on the risks you included in your risk framework (from step 2).

Step 3: Set up or update your risk assessment and proportionate response framework and import your data. The next step is to quantify the risks per relevant risk type and to assess and formulate the specific mitigants of each of the material risk drivers. To do so, an RSP should start by revising and updating its risk assessment matrix, ensuring that it has most of the following aspects:

- A list of all relevant attributes

[36] A risk appetite statement is a statement that either describes risk types, factors or attributes or a combination in a way that pronounces on the kind of risks the institution is willing or unwilling to undertake in its business. It can also describe activities or instances where the organisation cannot enter into certain business relationships or activities. For example, in its risk appetite statement an institution may note that in its remittance business it will have enhanced due diligence on politically exposed persons (PEPs), as well as customers from FATF greylisted jurisdictions. It may flag that it will not do business specific PEPs (e.g. former Presidents), weapons-based businesses, and customers from specific jurisdictions. That sets the risk appetite that should then inform risk assessment and rating. It implies, for example, that a customer sending remittance from greylisted country will automatically be rated as high risk and enhanced due diligence applied.

- The risk weighting of these attributes
- The existing risk mitigation approach to each
- The effectiveness of each of the mitigation strategies

For an example of a risk assessment matrix, please see Deep dive 4: A practical addition to the risk assessment intervention. This deep dive is beneficial for new market entrants, as it provides step-by-step support for RSPs on how to create the matrix, how to complete it and how to analyse it, as well as tips, tricks and best practices. Experienced RSPs can leverage the deep dive as a completeness check for how to conduct a risk assessment. They can use the matrix to identify areas that can be enhanced and benefit from the tips, tricks and best practices provided.

Once the risk matrix is done, it is essential to **import your own data** into the risk assessment. Incorporating your own data allows you to (1) validate the model; (2) ensure accuracy and relevance which supports a tailored analysis; and (3) strengthen your compliance process. Box 3 below provides a guide on how to incorporate data into your risk assessment while highlighting specific data groups to consider in your assessment process.

BOX 3: A guide – how to incorporate data into your risk assessment

- Regarding data driven risk assessments, a key **starting point** should entail an **audit of internal data** and research into **external data** and information sources.
- **External data** sources will include publications and industry statistics (e.g. Central Banks, Ministry of Finance, Banker's Associations, Department of Justice, a national cybersecurity centre, remittance associations, the FIC or FIU, national risk assessment, regional FATF publications and confidential non-published statistics on portals, or from the national statistics bureau, etc.). Examples include data on the average number of cases and convictions for predicate offences, particularly those that are related to ML-TF-PF, fraud, white-collar crime and corruption; information on IT ransom- or financial cybersecurity attacks; information on fines that regulated supervisors have extended to other regulated institutions that are in the public domain;[37] information on foreign exchange manipulation and -fraud related cases; and data on how remittances are being used to facilitate ML-TF-PF, etc.[38]
- **Internal data** allows you to understand your exposure to the national risk context. It entails mapping all the transactional and operational data dimensions and attributes that have a bearing on risk drivers or attributes. This includes transactional data and historical aggregated information from your banking or accounting systems, as well as information from inward IMTO files. Due to system setup for transaction efficiency, some important risk information is often not processed from IMTO files to internal systems or is aggregated into formats that complicate data analysis for the RSP.
- **Important information** includes sender and receiver personal attributes or identifiers such as national ID numbers, names, middle names, dates of birth, gender, town of birth, senders and receivers' alternative contacts, relationship and sub-reasons for the transaction.

- Where possible, data on marginalized groups such as **rural customers** should be leveraged. If such data is not available, RSPs can create proxies, for example using branches in rural areas as proxies,[39] looking at the reason for sending remittances, or when remittances are received during critical agricultural periods, as this indicates the dependence on the agricultural value chain. For a **gendered perspective**, where gender-disaggregated data is unavailable, name recognition software or sex indication on ID documents can be used to identify women in efforts to advance women's financial inclusion. Data on **lower-income people** can be identified by more frequent transactions (e.g. weekly when their remitters get paid), transactions received at particular times (e.g. before religious holidays, at the start of school terms, or critical agricultural periods like sowing and ploughing), those who receive remittances only during catastrophic events like flooding or droughts, or frequent transactions where low average amounts received, e.g. less than US$200.
- Once you have located the most important dimensions and data, the **next step** in data analytics is to determine a **statistically relevant sample**. For institutions with less than a million remittance transactions per month, it will be advisable to analyse all of it per month, which would provide a sound empirical base to make definitive risk analyses.
- The **period of the analysis** is also important to establish seasonal transactional norms and trends and usually ranges from a minimum of one year to a five-year period.
- Risk analyses should, finally, be **iterative** as new data are found and deeper analytics are possible. This will affect the risk attributes that can be evaluated over time and those that can be validly excluded based on evidence on undetectable risk or non-applicability based on solid data over time. Searching and evaluating the data is valuable in that it can reveal additional latent risks or mitigants and particularly behavioural norms that should colour the risk rating. E.g. a surge in payments and average value at key times could be normal and at other times could point to risk.

Generally, conducting a risk assessment and developing proportionate responses should be ongoing. It is best practice to conduct a comprehensive assessment every 12–18 months, or when there are significant changes in regulations, mergers, or the launch of new products or new jurisdictions, among others.

Step 4: Use your updated risk assessment matrix to enhance your business. With your risk assessment matrix finalized, you are now in an ideal position to take the next step towards achieving your objective (whether that be to just assess your risks, introduce a pre-determined innovation such as simplified accounts, or introduce innovative solutions to some of the challenges you may have picked up through conducting the risk matrix assessment). Understanding your risks and where you should go deeper or lighter, is a key part of generating new customers for your product and developing new products for your customers. This risk matrix should be seen to an end. Essentially, it is an effective business tool which can allow you to reduce compliance costs. It enables you to have a different type of risk appetite and should therefore be frequently updated and treated as a living document.

[39] An approach if you do not have to highlight the main branches in the urban areas, and everything else can be classified as peri-urban, or rural areas. Again, this should be checked with the country context and remove anomalies.

Step 5: Develop an action plan to implement changes from the risk assessment. Once you have determined the changes you wish to implement based on the outcome of step 4, you can prepare a plan to implement changes or to comply with the new systems to be put in place. The plan needs to set out who takes responsibility for various aspects (for example, updating and consolidating data could be done by an IT specialist, with coordination from the compliance team), and develop timelines for implementation. If capacity is constrained, you can focus on empowering risk champions across the different departments and branches. During the RAI programme, participating RSPs found that it proved valuable to appoint a risk and compliance staff member to oversee the implementation of activities. Ultimately, management and the board must take overall responsibility for implementing the changes.

Step 6: Empower staff for implementation. The steps above should feed into a training process to ensure that staff are trained on the changes. Training should not only be confined to staff but also to management and the board of directors. Training is a key pillar of an effective AML/CFT programme and a key control. During the RAI programme, it proved vital to empower branch staff by way of training to ensure that they implement the amended process(es) appropriately. This included providing them with sufficient background information about why the process changed so that they could maintain trust with clients and provide them with accurate answers to their questions or with additional information as needed.

> **TIP** Take care to clearly detail why changes to the risk assessment and proportionate response process is made to all staff who will be working with the updated process frequently. This is to reassure staff that the necessary safeguards have been put in place to mitigate risk and highlight their role in identifying suspicious transactions or customers. Simultaneously, it is crucial to destroy all old process documents and blank forms and re-engineer workflows to exclude the obsolete processes.

KEY LESSONS REGARDING THIS INTERVENTION

Based on the experience of the RAI programme there are a few key lessons to be on the lookout for when implementing a risk assessment, from an institutional as well as an implementation perspective.

LESSON 1 **Get top management buy-in early on.** It's important to have managerial buy-in to AML-CFT and risk assessment processes to ensure that they are aware of the risks, that they can take informed decisions on how to address and prevent these, and to allow them to use the insights to inform strategic business decisions.

LESSON 2 **Build in data skills.** Most RSPs do not incorporate data into their risk assessment. This is due to limited data availability and data analysis capacity which impede their ability to manage risk and innovate to enhance remittance access. Having a dedicated data analyst assigned to the intervention, who is skilled in Excel and Power BI, for instance, can assist in ensuring that the system can provide data to be filled for risk assessment purposes.

LESSON 3 **Engage outward.** A change in an RSP's risk assessment approach (e.g., to follow a data-driven risk-based approach) requires engagement with the broader market and regulators. This is to ensure that you are (a) following best practice, or in the case that you are a "first-mover" in this space, (b) that you are providing evidence as to why this approach is more effective.

LESSON 4 **Systems integration.** There may be some work required to integrate different systems and databases, especially between your sub-system and that of the IMTOs. This may require some development but should not result in too many significant delays. You can plan for this in your timelines, after conducting the pilot and identifying glitches. Having someone skilled in IT or development could easily solve these issues.

LESSON 5 **Leverage learnings.** Ensure that you get the most out of your risk assessment by using the data that feeds into it to inform other marketing opportunities. Remittance data can provide rich information about a customer's transaction behaviour, when they get paid and in which markets, they operate. This can allow you to better target them for other products and services, based on their behaviour as gauged from the data.

TABLE 12: DOs AND DON'Ts OF THE RISK ASSESSMENT

✓ Dos	✗ Don'ts
Have introductory meetings with all key stakeholders, and then have a kick-off meeting in which you discuss the implementation plan, timelines and key responsibilities	Don't leave stakeholder engagement (e.g. IMTOs, partner organizations) to the last minute
Have meetings with management to secure their approval for the intervention and for key points of access. For example, ensure that management approves your access to relevant data sets and is aware of where in the project they will need to make key decisions	Don't start the process without managerial approval and buy-in
Involve the relevant teams to capture accurate information. For example, business, compliance, etc. This also speaks to the methodology of risk assessment in your organization. The best practice is to do it bottom up, whereby frontline units/ entities' risk assessments feed into the legal entity/business line and ultimately the enterprise. The stages vary with the type and structure of organizations. For example, smaller organizations without several departments and units may just have an enterprise risk assessment	Don't complete the risk assessment without the relevant units/entities
Ask the regulator for clarity if you are unsure about changing your processes and seek out their feedback after making the system changes. This heavily depends on the regulatory approach in your jurisdiction and the extent to which its rules vs principles based) Also flag these changes and plans in your regular catch ups with the regulator. Where these don't happen as often, then proactively inform, and seek input and feedback from the regulator as may be relevant	Don't leave the regulator in the dark
Start small. A risk assessment tool in Excel, that has live data fed into it, can be a great starting point	Don't think that you must undertake large-scale system changes to make the intervention successful
Make use of data as much as possible in your risk assessments. Data driven risk assessments are more credible and effective. They also enable management and boards to make better decisions than perception-driven assessments	Don't persist with risk assessments that do not prioritize the utilization of data
Enable your compliance department to access remittance data to inform the risk assessment, as needed	Don't make data access and use a challenge for compliance and related departments

MEASURING YOUR SUCCESS

Assess the success of your risk assessment and proportionate response intervention by measuring appropriate success indicators. Impact measurement should not be an afterthought, it must be built into the intervention plan from the start. The first step for impact measurement is developing the success indicators based on the objective(s) that you identified at the onset of the intervention. The second step is then to determine how you will measure these indicators, that is what data you will collect, over what period and what kind of insights you would like to draw from this. Table 13 below provides an example of the type of indicators that can be developed based on one potential objective of the risk assessment matrix:

TABLE 13: EXAMPLE INDICATORS FOR MEASURING SUCCESS OF MEETING OBJECTIVE

Set objective	What to measure	Indicators (data to collect)
Enhance remittance access for low-risk persons.	Customers subject to less stringent due diligence requirements	• Number of customers now rated as low risk. • Number of customers no longer required to provide additional documentation. • Number of customers moved between risk rating tiers. When taken together, the enhanced efficiency indicated by the above indicators will assist in calculating the overall decreased cost of compliance. *Note: where possible, these indicators should include references to the SDGs, as when people are engaged in the economy, they can become more prosperous and have increased activity which can benefit your organization. Data should also be segmented by e.g. urban/rural, age, gender, etc. to gain a better understanding of your customer base and thereby ensure that risk profiling is more accurate*

An easy way to measure whether the indicator(s) have been met, is to compare the system data that informed the adjusted risk ratings with more recent data collected during and after implementation.

FUNDAMENTAL CONSIDERATIONS REGARDING RISK ASSESSMENTS[40]

As financial sectors, services, and technologies emerge and advance, so do the types of risks associated with each. As a result, you must continually update and improve upon your risk assessments and proportionate responses. This section concludes the risk assessment discussion by recapping the fundamental considerations necessary to ensure that the risk assessment and risk responses remain effective in ever-changing realities well after you've implemented the intervention above.

Start with the end goal in mind. The first consideration when taking on a risk assessment is to set the strategic objectives for the assessment, that is, what is

[40] In addition to this, Cenfri is part of an initiative, working with other stakeholders, focused on developing risk principles to enable better implementation of FATF recommendations. These fundamental considerations provide a basis for the discussion on the risk principles

to be achieved. This will set the tone for how you design your risk assessment framework, determine the information and data you collect and insert, and inform your thinking about the intended outcomes. The intervention checkpoint in sub-section 3.1.1 provides a guide for RSPs on how to set their objectives. **Deep dive 3: A guide for regulators to assess regulations against inclusive integrity goals and best practice** guides regulators on how they can set their inclusive integrity goals.

Adopt an outcomes-based approach. A common pitfall for institutions is focusing on the output of a risk assessment instead of the outcomes. This is because a focus on *outputs* will indicate how risk ratings have changed, whereas focusing on the *outcomes* will indicate the extent to which risk has been mitigated. The latter is therefore a more indicative and informative indicator of the success of a risk assessment and proportionate responses. The risk assessment framework proposed in this toolkit, in "A step-by-step guide to implementation" above, is a simple yet effective data-driven risk assessment model which encourages the shift to an outcomes-based approach to managing risk.[41]

Disentangle interrelated risks. Throughout this toolkit, emphasis is placed on the need to understand risks, and specifically how they affect the remittance business. In addition to understanding and defining risks, it is also crucial to understand how the risks are interlinked to avoid unintended consequences when mitigating each. The definitions of these risks and guidance on how to disentangle the various risks when assessing each is discussed earlier in this chapter.

Data-driven risk assessments. The risk assessments should move from mere perception-based statements to data-driven assessments. This helps compliance officers to align expectations in conversations with their board of directors, management as well as regulators. The use of both qualitative and quantitative data is encouraged to support and back risk assessment, ratings and control decisions.

Risk governance. The governance of AML/CFT risk is key to its management. This means that the roles and responsibilities of the various role players should be clear. This includes but is not limited to compliance officers, management, the board of directors and various committees (such as the AML committee, the audit committee, the sanctions committee, etc.). This is a significant step in ensuring that each player is held accountable for their role. Risk governance is therefore a key piece in risk management and overall governance.

Measure what matters. The old saying, *you cannot manage what you do not measure*, also holds for risk assessment and management. To design the correct mitigation measures to manage risk, you should prioritize the collection of practical and relevant measures that go beyond compliance, i.e. avoiding collecting indicators as part of a "tick-box" approach merely to avoid the risk of fines. Instead, the organization should understand the consequences of poor

[41] An example of the model is discussed in Deep dive 4: A practical addition to the risk assessment intervention

risk management, like the potential loss of customers through disproportionate KYC and CDD practices to encourage sound risk management. Therefore, risk measures should serve a purpose, be practical and relatively easy to collect and should be used as living inputs to continually assessing and ultimately managing risk.

Join the conversation to transform your risk assessment and proportionate responses. There is an ongoing dialogue among financial sector regulators, supervisors, and market players on what effective risk assessment and proportional responses should look like, consider and achieve. Participation in these conversations is an essential part of keeping your risk assessment and proportionate responses in line with best practices, positioning it to strengthen your competitive advantages and enhance your compliance. The considerations above should equip you to start this discussion within your organization and between industry stakeholders.

3.2 Digital ID database

The second intervention entails developing a digital ID database for walk-in or over-the-counter customers. Based on the Remittances Access Initiative experience, this is one of the interventions that RSPs are most in need of.

INTERVENTION CHECKPOINT

What can you do when customers forget or have lost their IDs? In most jurisdictions, it is a requirement for customers to bring acceptable forms of ID to the RSP to receive their remittance. However, a common challenge is that people show up at RSPs without an ID (because it's been forgotten or lost) or with a damaged ID. As a result, frontline tellers are not permitted to serve these customers, and in many cases, the cost of going back home to fetch an ID or to get a new ID is prohibitive. Subsequently, some customers just do not come back to fetch their money. This KYC barrier therefore incentivizes customers to use easier but more insecure informal channels. To address this challenge, there is an opportunity for the RSP to keep a copy of a customer's ID. The simplest way to do so is to keep a digital copy on a digital database.

A digital ID database enables RSPs to serve recurring customers by leveraging a digital copy of their national ID. A digital ID database is a crucial step in any RSP's digital transformation journey. It entails (1) setting up a digital storage facility, which can be on your server or a cloud-based server like SharePoint; and then (2) enabling frontline staff to save digital copies of customer IDs on this digital storage facility, which can be done by allowing frontline tellers to make a copy of the front and back of a customer's ID using traditional computer scanners or hand-held devices.[42] Once a copy has been taken, the frontline teller will save a copy onto the database with a unique code (e.g. a customer's ID number). In practice, this would allow frontline tellers to verify the recurring

[42] Hand-held devices can be especially useful if IDs have a barcode. This is most useful if the barcode is linked to a national database for verification.

customer's identity (for whom you have a saved digital ID) using a variety of other photo-bearing identifiers. For example, if a customer comes into the branch and has forgotten their ID, but you have a copy of their valid ID on your system, then your frontline teller validates the customer by sending a One Time Password (OTP) to the captured mobile number. When using any methods of capturing the customer's ID, the necessary precautions like access controls, password protection and safe recordkeeping should be followed.

An intervention to convert OTC customers into regular customers. In most jurisdictions, KYC and even e-KYC have a face-to-face component. This intervention seeks to turn OTC clients into regulars given the convenience factors, particularly since sending away many customers daily poses a reputational risk. This holds significant business cost savings, as RSPs will have to conduct KYC only once per client.

There is an opportunity to enhance this intervention by creating customer profiles. The digital ID database allows the RSP to simplify the KYC and CDD process. This can be significantly enhanced by creating a unique profile for each recurring customer on the digital ID database. This is explored as a standalone intervention in section 3.3 but is also worth mentioning here, as the digital ID database is the foundation for digital ID proofing. Customer profiling starts by collecting basic information (name, age, ID number, etc.) and saving it alongside a copy of the customer's ID. Each time the customer comes in to collect or send remittances, their transactions are automatically captured and tracked in their unique profile. Over time enough data is collected to derive insights on customer behaviour which can then be leveraged to offer them a variety of formal financial products. For example, if proven to be low risk, there is an opportunity to offer them a tiered account even if they do not have all the necessary KYC and CDD documentation (such as proof of address, signed letters from husbands or fathers, and so forth). This would enable the RSP to develop targeted interventions to better serve their existing customers and to attract new customers, specifically people who are using informal channels or leveraging other providers, through an improved and competitive product/service.

An introduction to digital identity proofing

Digital identity proofing refers to the continuous identification and verification process which digital identity systems conduct. This is done by using additional data collected during authentication (such as transactional data combined with GPS and IP address data) to continuously update and strengthen the identity profile (Cenfri, 2020). Employing digital identity proofing enables remote onboarding which allows you to reach remote and rural customers and expand your customer base. Furthermore, this also enables more appropriate risk management, as an up-to-date, accurate profile can more easily be assigned proportionate risk management controls.

Before you dive in, weigh up the costs and benefits. To determine whether this intervention will be worthwhile, it is important to start by comparing the costs and benefits associated with implementing the intervention. The table below provides a guide for how you can think about estimating the costs and benefits of the intervention within your context.

TABLE 14: COSTS AND BENEFITS OF THE DIGITAL ID DATABASE INTERVENTION

Benefits

Increasing the customer base and enhancing the customer experience

- Improves convenience for customers as it saves them time and saves them a trip back home if they've forgotten their ID.
- Allows customers to retain access to their finances even if they have lost their ID thus giving them comfort and uninterrupted financial agency.
- Gives customers the freedom to bring in alternative identifiers.
- Creates customer loyalty and a customer relationship that does not depend on an account-holding relationship.
- Enables growth in the customer base without compromising the KYC risk-mitigation measures.
- By increasing your potential customer base, you can also increase your revenue base.
- Reducing the risk of rejected or abandoned transactions. The digital database reduces the chances of a customer not being able to collect their remittances due to not having their national ID.

Improving business operations

- Increased digitalization – automating a manual process.
- Reduces the risk of human error.
- Improves business efficiency by improving process flows and reducing time spent on explaining acceptable identity requirements to customers
- Reduced KYC and CDD onboarding and screening i.e. single onboarding process per customer instead of KYC and screening per customer per transaction.

Strengthening KYC and CDD compliance

- Empowers the RSP to demonstrate a high level of overall effectiveness in ML-TF risk management. It can also reduce the overall AML/CFT and compliance costs since the system can use data and feed into risk assessment and management frameworks.
- Enables you to conduct continuous CDD on customers throughout the lifecycle of the relationship.
- Reduces AML/CFT risk. Digital identity systems typically rely on more robust methods for identification and verification than traditional manual systems. In addition, the database allows you to continuously conduct CDD on customers using the same identifier that you have throughout the lifecycle of the relationship. This allows you to gradually build up and strengthen a customer profile which can later be used for identity-proofing. This also makes it more difficult for customers to use fraudulent IDs or IDs that are not theirs.

Costs

Internal time and capacity needed to assess the options available for a digital ID database, assess the compatibility with existing systems and manage the digital ID database project (including stakeholder coordination, piloting etc.

Outsourcing or leveraging an external/internal IT or software developer. An IT expert will be needed to develop the digital ID database with the requisite requirements.

System-change related costs if the existing system does not have the functionality to host a digital ID database. This includes the cost of acquiring scanners, barcode readers and other devices which can make copies of customer IDs if not already available.

Depending on the state of your system, there may also be system-change related costs associated with shifting from a manual to an automated system. These include for example digitising existing paper-based records, training your staff, or marketing for customers. In the future, there could be costs associated with improving the quality and speed with which the digital copy is taken and stored. For example, complementing the scanner with a webcam to capture high-resolution images of customers, or raising expenditure on preventing cyber-attacks, hacking, etc.

Getting ready – key considerations when implementing this intervention

- **Time:** roughly 6–10 months from design to implementation. This is estimated based on the assumption that you will have managerial buy-in and no approval or technical delays.
- **Capacity:** a project champion who will be responsible for managing the implementation of the intervention. In addition, you will require someone with software development and system management skills, who will oversee the actual development and implementation of the database. This person will be crucial to ensure that your database is interoperable with your existing systems.
- **Key dependencies:** alignment with IMTOs to ensure that they are aware of the intervention and how it can change documentation requirements, as well as ensuring that there is system interoperability with that of the IMTOs. This is relevant for any remittance service provider that's partnering with IMTOs.
- **Regulatory considerations:** consider the regulatory assessment for your country, specifically drawing on the AML/CFT Act, regulations, guidelines. Key things to consider includes the types of IDs you can collect, the storage requirements, how to identification documents should be verified, etc.

What success can look like – testimonial from the RAI

Ecobank Uganda implemented the digital ID database intervention. They shared the following feedback:

- "The intervention has **improved our turnaround time**, thus optimising front office efficiency".
- The intervention has also resulted in **improved customer experience**.
- The intervention provided a suitable environment for **seamless traditional product cross selling**.

They have the following implementation advice for others interested in implementing this intervention: Consider incorporating external resources for system development activities. In addition, ensure that all internal stakeholders are engaged to avoid delays across the project stages.

Ecobank is a pan-African remittance service provider, with banking operations in 33 African countries, including Ghana. It is the leading independent regional banking group in West Africa and Central Africa and serves both wholesale and retail customers.

A STEP-BY-STEP GUIDE TO IMPLEMENTATION

Step 1: Involve the necessary teams and expert opinions early on. To ensure that you are compliant with all the necessary regulations and that the changes that you wish to implement are practical and possible, you will need to involve various experts at different stages of the intervention. It is important to involve an IT system developer who can advise on (1) developing your internal database and (2) compatibility and systems interoperability – for example, if you want it to be interoperable with your other systems, or even interoperable with national systems (where available) to simplify the verification process. This expert can be external or internal and will be brought in to evaluate the final system changes once completed. It is also important to involve your relevant internal teams such as your IT, risk and compliance teams.

Step 2: Determine how you will collect ID copies. Once you have received the experts' opinions on how you should set up your systems, you will have to determine how you intend to capture digital ID copies. This will include determining which tools you prefer to perform this function. For instance, to capture the copies, handheld scanners, computer scanners, or designated mobile phones are needed within the organization. These copies will need to be in a compatible format for your system (e.g. in JPEG or PNG format) and be taken in colour to capture all the relevant details on the ID, as well as on the picture. Ideally, there is an opportunity to have a scanner-based app built into your system so that it reads and populates the digital ID databases' customer page with the relevant information from the ID copy. In this step, you will also need to consider how you will collect ID copies via remote onboarding options, e.g. via agents, and via application programming interfaces (APIs) used outside of a branch environment.

Step 3: Develop/set up your database. Start by selecting or developing a centralized database which will house the digital ID copies. You can choose between developing your database or using software like *SharePoint* to host your database.[43] It will also be important to refer to the regulatory assessment and see if there are any specifications on where you must store your data. In many countries, data on customers must be stored within the country, which may limit the ability to leverage alternative cloud-based sources and servers. During this time, you should also identify the type of information that you want to store.

Once you have determined the *how* you must determine the *what*. This means creating a succinct and non-onerous list of customer details you intend to collect. Key points to collect include customer name, date of birth, sex and ID number, as well as ID type, issuing authority, issuer (country), ID issue and expiry date. Table 15 below indicates the specific requirements for the digital ID database.

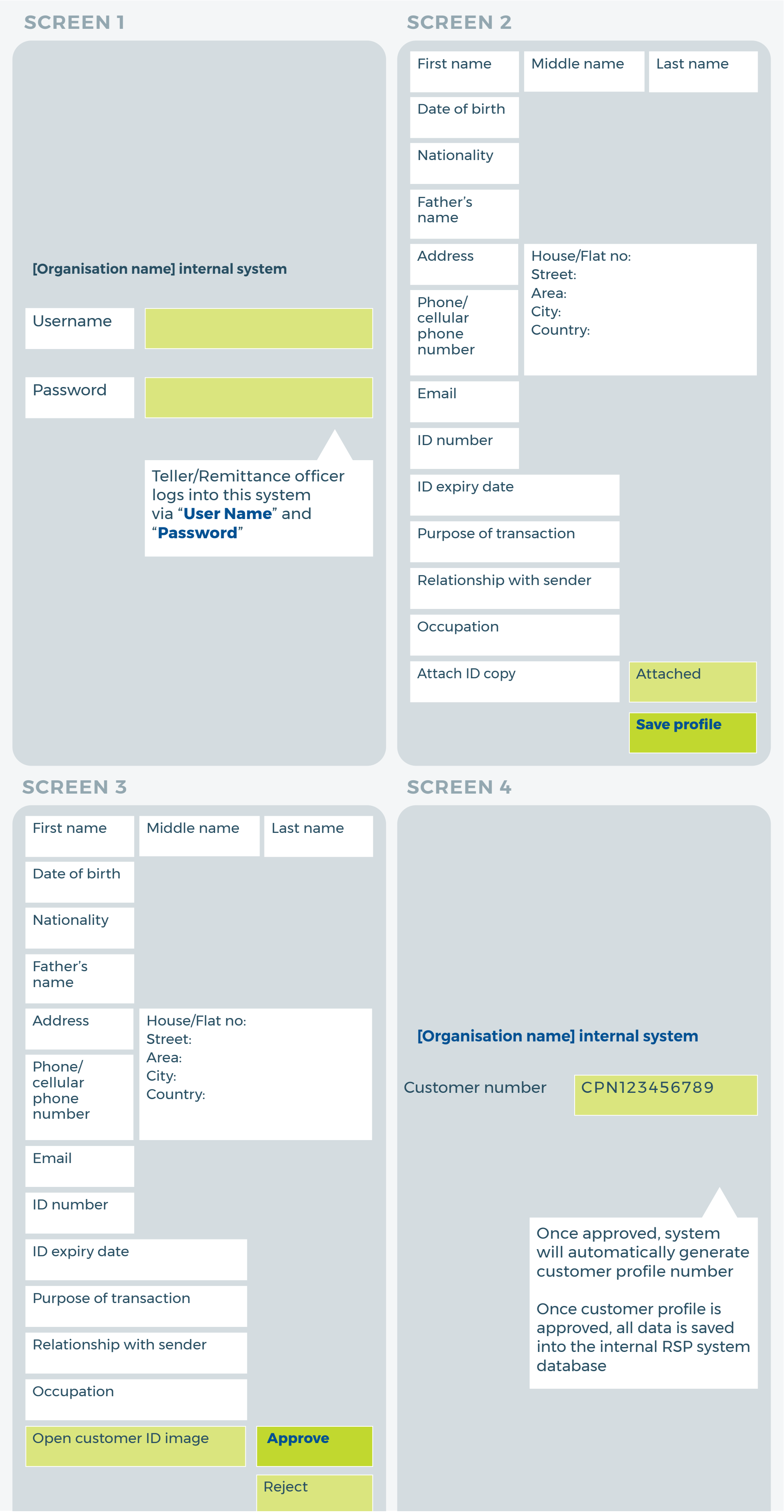
[43] Other databases can also provide similar support, like ID123 (ID123, n.d.). The most important requirement for any database or system that you incorporate, is that it should be interoperable with your existing system and that it should not require duplicate efforts from staff.

TABLE 15: DIGITAL ID DATABASE STORAGE REQUIREMENTS

Digital ID database storage requirements	
Storage Type	Cloud or SharePoint or any other appropriate storage
Storage Size	The years of data that can be stored and accessed should comply with the data retention period required by law. This usually varies from 5 to 10 years.
Storage Specification	The database should be accessible by authorized staff from their desktops only so that log-in and use can be tracked to prevent fraud. Authorized staff members should be provided with a unique username and password [The company data and access hierarchy policy and process specification documents would need to be updated and approved according] If your organization employs remote onboarding, the system should include API uploading from agents who are often based in rural areas.
Storage design	The storage design should ideally include: • A log-in screen, a home screen and a screen for each customer profile • The home screen should have search options (Full Name, Phone Number, ID Number etc.) and only bring up the customer profile for the unique code entered (in other words a frontline teller should not have access to the entire list of customers upfront, only to the customer that has provided their unique number) • The customer screen should have an allowable size for each file, a permitted format of each file (jpeg or pdf format, etc.), a required file name, a file and a customer record update option • Ensure that a file can be replaced while keeping the old version on record • Customer files to be stored in chronological order

Typically, your database should end up looking as illustrated in figure 3 below:

FIGURE 3: ILLUSTRATION OF DIGITAL ID DATABASE INTERFACE



SCREEN 1

[Organisation name] internal system

Username

Password

Teller/Remittance officer logs into this system via “**User Name**” and “**Password**”

SCREEN 2

First name | Middle name | Last name

Date of birth

Nationality

Father’s name

Address

House/Flat no:
Street:
Area:
City:
Country:

Phone/ cellular phone number

Email

ID number

ID expiry date

Purpose of transaction

Relationship with sender

Occupation

Attach ID copy | Attached

Save profile

SCREEN 3

First name | Middle name | Last name

Date of birth

Nationality

Father’s name

Address

House/Flat no:
Street:
Area:
City:
Country:

Phone/ cellular phone number

Email

ID number

ID expiry date

Purpose of transaction

Relationship with sender

Occupation

Open customer ID image | **Approve**

Reject

SCREEN 4

[Organisation name] internal system

Customer number | CPN123456789

Once approved, system will automatically generate customer profile number

Once customer profile is approved, all data is saved into the internal RSP system database

Step 4: Set up appropriate security standards and procedures. The digital ID database and ID copies are only one part of the process. For this system to work effectively and efficiently, it needs to be complemented with appropriate security protocols. This includes limiting the use of frontline tellers to uploading and viewing customer pages; ensuring that only managers can delete and change customer pages; and ensuring that these pages remain up to date. Table 16 below details additional security features to build into your digital ID database once the two components have been connected.

TABLE 16: ADDITIONAL SECURITY FEATURES TO BUILD INTO THE DIGITAL ID DATABASE

Digital ID database additional security features	
User management specifications	To ensure the safety of customer data, you will prepare a user management process that includes but is not limited to: • Username structure • Password structure • Password reset policy • User management department • Viewing and editing rights • Furthermore, if requested by law enforcement or a central bank, special authorization must be provided to a compliance department to download an ID copy • Ensure that the user account is logged off after 3 minutes of inactivity (note that this is an indicative time; it may vary based on the specific RSP's requirements) • A background screen, only available to management, should log and trace the activity of each frontline staff member and flag any errors and discrepancies
Storage access	• Only authorized staff can access the storage • After entering the username and password, the authorized person can use several identifiers to locate the ID • The ID image can be opened in several sizes • ID image cannot be stored, nor copied or downloaded
ID scanning	Authorized staff scans the ID that will be automatically stored on the database. A process flow needs to be designed.

Step 5: Integrate relevant flags and notifications. Based on the specific RSP's context and preferences, there are a variety of additional and "nice to have" features that can be added. These add-ons serve various purposes, including added safety and security when using the database and working with customer data, as well as other user experience improvements. Examples of add-ons include:

- A one-time PIN (OTP) to verify that the customer is who they say they are to reduce fraud. Various requirements can be built into this feature, including an expiration window for this OTP to ensure that it is used for the correct transaction each time.
- Notifications to flag to the customer a month before that their ID will be expiring soon, in instances where IDs expire
- Additional fields to support risk analytics and understanding customer behaviour, for example, a "type of transaction" field

- Colour-coding error messages, e.g. by changing boxes and pop-ups to red to differentiate from normal system notifications. This can prevent tellers from mistakenly serving a customer
- Timers to each page, which log the user out after a determined period of inactivity to prevent unauthorized access (e.g. five minutes)
- Setting up unique login and password details for all front-line staff
- Updating the system to allow for two types of administrators. These are: 1) those that can input information (e.g. a teller); and 2) those that authenticate inputs to the system (e.g. compliance staff)
- Introducing ID and document watermarking to prevent identity theft through screen photographs by staff, tellers and users
- Incorporating audit trails into the system design to track teller usage and activity on the system

Step 6: Train frontline staff. Staff buy-in is central to the smooth implementation of this intervention. You will need to prepare your staff for the imminent changes to their processes. This is done first by training front-line staff members. The best way to do this is to develop a training manual which includes at least the following elements: (a) what the intervention entails; (b) the benefits of the intervention; (c) changes to the remittance receiving process both for the RSP and the customer; and (d) what the changes will look like in practice. These materials can also be used as a way of documenting changes for future staff members. In the training session(s), ideally include branch managers, customer service representatives, front-line tellers and compliance staff and cover the materials included in the training manual. Finally, include a live demonstration of how to use the system in the training.

Step 7: Sensitize customers to the new process. The next step is to sensitize customers to the upcoming changes to their customer journey. This can be done by developing posters to place in branches that depict how the customer journey will change for new and recurring customers. This can be complemented by targeted marketing campaigns to the existing and prospective customer base (e.g. via SMS blasts and brochures) to inform customers of the system changes. In addition, place customer service representatives in branches who can support customers with the new process in the first few weeks of implementation.

Step 8: Pilot the intervention. To test how the intervention lands with staff and customers, it is important to launch a pilot test. This step is crucial to ensure that any glitches are ironed out before the intervention is rolled out large-scale across all branches, and to ensure that the intervention is having the desired effect. To pilot, you could select 2–3 three key branches in different regions. The customer base in these selected branches should have a good combination of rural and urban customers, as well as men and women to ensure that you get a good grasp of how the intervention will work with various aspects of the customer base. Next, start with the training and sensitization of the intervention, as covered in Step 6, for one month. Thereafter, roll out the pilot process for 2–4 months to conduct user acceptance tests (UAT). During this time, record and analyse the data, and identify and address any bugs that may come up during the pilot. It is advised to document each test conducted, for example inputting the wrong login details, to show what the expected and actual results are, as well as the status of each test (pass or fail). If the bugs are significant and you require more time to test the efficiency of the system in practice, consider continuing the pilot for another three months to further collect data.

Step 9: Roll out the intervention. After ironing out any glitches in the system, you are ready to roll out the intervention to your branches. The pilot may need to be repeated during implementation to encourage uptake of the intervention during implementation, it may be good to repeat step 1 as well, to determine what the customer and staff feedback is. Based on the feedback, you can identify new opportunities for your organization and determine which aspects require improvement.

KEY LESSONS REGARDING THIS INTERVENTION

LESSON 1 **Implement the intervention with internal products first.** Rolling out the intervention with an internal product reduces time delays due to partnership agreements and obtaining sign-off from, for instance, an IMTO. Once the benefits are clear and the solution has been verified it will be easier to convince other partners to implement a similar intervention.

LESSON 2 **Know where your customers are at in terms of digital and financial literacy.** If you implement innovations like using an OTP to verify a customer's identity, you will need to be sure that most of the customers have access to a mobile phone. If not, you may have to consider other means of (manual) verification.

LESSON 3 **Be prepared to overcome intervention adoption hurdles.** To ensure the success of the intervention, you will need to be determined to overcome any challenges related to buy-in and intervention adoption. This will entail changing customer and staff's mindset, e.g. conducting many training sessions, sending daily reminders about the process change and tracking the progress of the intervention to boost staff morale.

Further tips on basic dos and don'ts are provided in Table 17 below:

TABLE 17: **DOs AND DON'Ts OF THE DIGITAL ID DATABASE**

✓ Dos	✗ Don'ts
Account for select cases where a manual process may still be required, e.g. if customers cannot verify their identity via an OTP because they do not have a mobile phone	Don't assume that you can completely do away with the manual system
Consult the regulatory framework and regulator on recordkeeping and data privacy requirements when saving a digital ID copy on your system	Don't forget about data- and privacy laws
Proactively mitigate risks like ensuring that you serve the right customer by authentication methods like OTPs	Don't disregard the potential risks
Look ahead at how you can use this database for other parts of your business, e.g. building a transaction profile, targeted marketing, etc.	Don't stop with implementing only the digital ID database

MEASURING YOUR SUCCESS

Developing key indicators to measure your success. The next step before launching this intervention, you need to determine what your key indicators of success are. These indicators will be based on the challenges that you identified during the planning stages of this intervention, e.g. KYC challenges related to not having the correct ID document. Key indicators to measure include:[44]

- Number of OTC customers served
- Number of ID copies collected
- Number of customers served using digital ID copies
- Number of recurring customers
- Number of repeat KYC screenings for occasional or walk-in customers
- Average time spent on serving customers using the digital ID database
- Average time spent on serving customers requesting a physical ID

When taken together, the enhanced efficiency indicated by the above indicators will assist in calculating the overall decreased cost of compliance.

Collecting data and assessing the impact. To get an accurate measure, you will need to start data collection before the intervention is launched to form a reliable baseline. It is recommended that you use data over three calendar months before the intervention is launched and compare it to the same three calendar months after the intervention is active, to account for seasonal changes. For example, if you plan to implement the intervention in March of Year 2, you will need to collect data for March–May of Year 1, and then again for March–May for Year 2. This data can be collected on a simple Microsoft Excel sheet. As part of the analysis, you should conduct calculations like determining the growth in the number of IDs saved on the system. These calculations should be done both on a month-to-month basis, and a year-on-year basis to show the growth after implementation, as well as the comparison between pre- and post-implementation.

[44] Note: where possible, these indicators should include the SDGs, as when people are engaged in the economy, they can become more prosperous and have increased activity which can benefit your organisation. Each of the data indicators should be segmented by e.g. urban/rural, age, gender, etc. to gain a better understanding of your customer base, to expand reach and to ensure better product development and -offerings.

3.3 Remittance customer profile

INTERVENTION CHECKPOINT

This intervention entails creating customer profiles for all walk-in customers and using them to serve recurring customers. A customer profile is essentially a digital summary of a customer's identifying information and a track record of their financial transactions. The customer profile provides an overview of customer information (basic KYC) and allows the RSP to do once-off KYC (with regular profile updates and KYC updates) for over-the-counter (OTC) remittances. To make this process as smooth as possible, it should therefore also include a digital copy of the OTC customers' valid ID (to first set this up, see the previous intervention).

The customer profile intervention can be built from the digital ID database or can be a standalone intervention. As discussed under the digital ID database intervention; the customer profile intervention can be a useful add-on intervention to the digital ID database intervention. Both employ digital identity and identity proofing methods as their foundation, but the customer profile intervention offers the additional benefit of tracking customer behaviour. If you intend on implementing the digital ID database as well as the customer profile, you will have to start integrating the customer profile requirements from Step 3 of the implementation journey for the digital ID database. Progressive identity and authentication are actively encouraged by FATF (especially under FATF's digital identity guidance) as a way of addressing exclusion. Customers may be onboarded based on limited information, which will be progressively populated as their digital footprint (through transacting more) develops. Similarly, in instances of proven or suspected low risk, authentication and verification can be staggered and need not be done simultaneously with identification. This encourages financial inclusion and reduces the risk of excluding customers with a limited digital footprint at a point in time.

Before you jump in, weigh up the costs and benefits. To determine whether this intervention is worthwhile, it is important to compare the costs and benefits associated with implementing the intervention. The table below provides a guide for how you can think about estimating the costs and benefits of the intervention within your context.

TABLE 18: COMPARISON OF COSTS AND BENEFITS ASSOCIATED WITH IMPLEMENTING THE INTERVENTION

Benefits
Reducing fraud. Most (97 per cent) of remittances are received OTC, through cash-based services (World Bank, 2021). Such customers do not have formal transaction profiles linked to accounts, which often makes them mysterious and risky to FSPs. For many RSPs, these OTC customers raise several fraud risk flags (customers not using their own identifiers, etc.). The customer profile intervention cuts through this challenge by allowing RSPs to gain greater insight into OTC customers, verify their identities more reliably, and do so without asking these customers to sign up and open an official account.
Collecting simple KYC information as well as a copy of a customer's ID significantly reduces the chances of customers being able to present fraudulent IDs or IDs used by others because their information will not match what is saved on the RSP's database. This reduces the risk of fraud by keeping track of customer details. Reduced fraud will reduce costs to customers and to the organization as you will no longer need to reimburse the customer or be tasked with finding the person who committed the fraudulent activity. In addition, this intervention simplifies the KYC process for staff, especially on recurring customers, thereby reducing the chances of conducting KYC improperly.
Increasing visibility of the KYC process conducted by cashiers. This intervention will increase the pressure on cashiers by holding them accountable for creating a customer profile for each customer and using this customer profile for recurring customers. There is now an increased risk of being caught while not conducting KYC/conducting KYC improperly.
Identifying new opportunities by targeting customers for affiliate products based on their records and behaviour. By creating customer profiles, it is possible to track OTC customers by way of a unique number, or identifier, which builds a profile of their behaviour over time. For example, information on when customers transfer money, how often they send remittances or even which countries they transact with the most, can all provide indicators for how you can amend your product offering. This information can be used to develop new and more targeted products, even offering bundled products such as remittances coupled with insurance, savings products and even short-term loans.
Building loyalty. Finally, providing OTC customers with customer-related benefits, such as personalized service and even access to tiered accounts, can help to build loyalty.
Costs
Internal time and capacity needed to assess the options available for a digital ID database, assess the compatibility with existing systems and manage the digital ID database project (including stakeholder coordination, piloting, etc.).
Outsourcing or leveraging an external/internal IT or software developer. An IT expert will be needed to develop the digital ID database with the requisite requirements.
System-change related costs if the existing system does not have the functionality to host a digital ID database. This includes the cost of acquiring scanners, barcode readers and other devices which can make copies of customer IDs if not already available.
Depending on the state of the existing system, there may also be system-change related costs associated with shifting from a manual to an automated system. These include for example digitising existing paper-based records, training staff, or marketing for customers. In the future, there could be costs associated with improving the quality and speed with which the digital copy is taken and stored. For example, complementing the scanner with a webcam to capture high-resolution images of customers, or raising expenditure on preventing cyber-attacks, hacking, etc.

Getting ready – key considerations when implementing this intervention

- **Time:** roughly 6–12 months from design to implementation. This is estimated based on the assumption that you will have managerial buy-in and no approval or technical delays.
- **Capacity:** a software developer to design and implement any systems changes, as well as ensuring that staff are trained on the changes required in their processes.
- **Key dependencies:** alignment with IMTOs to ensure that they are aware of the intervention and how it can change documentation requirements, as well as ensuring that there is system interoperability with that of the IMTOs.
- **Regulatory considerations:** consider the regulatory assessment for your country, specifically drawing on AML/CFT acts, laws, regulations, directives and guidelines. Key things to consider includes the types of IDs you can collect, the storage requirements, etc.
- Further requirements for the customer profile build on that of the digital ID database, which can be found in A step-by-step guide to implementation.

A STEP-BY-STEP GUIDE TO IMPLEMENTATION

Step 1: Set up the platform and customer profile. To start this intervention, you can either set up a digital ID database, or you can create a space on your existing operating systems to create and save profiles for OTC customers. If you opt for the former, it will be important to ensure that this database is interoperable with your existing and future systems or technology. It is advised that the profiles you create, regardless of the platform, include the following information fields collected from customers the first time they come in:

- Customer data: full legal names, date of birth, ID number, gender and other customer data you may need
- Digital copy of customers' IDs (front and back)
- Transaction history, transaction dates, purpose of transactions, destinations, values, etc.

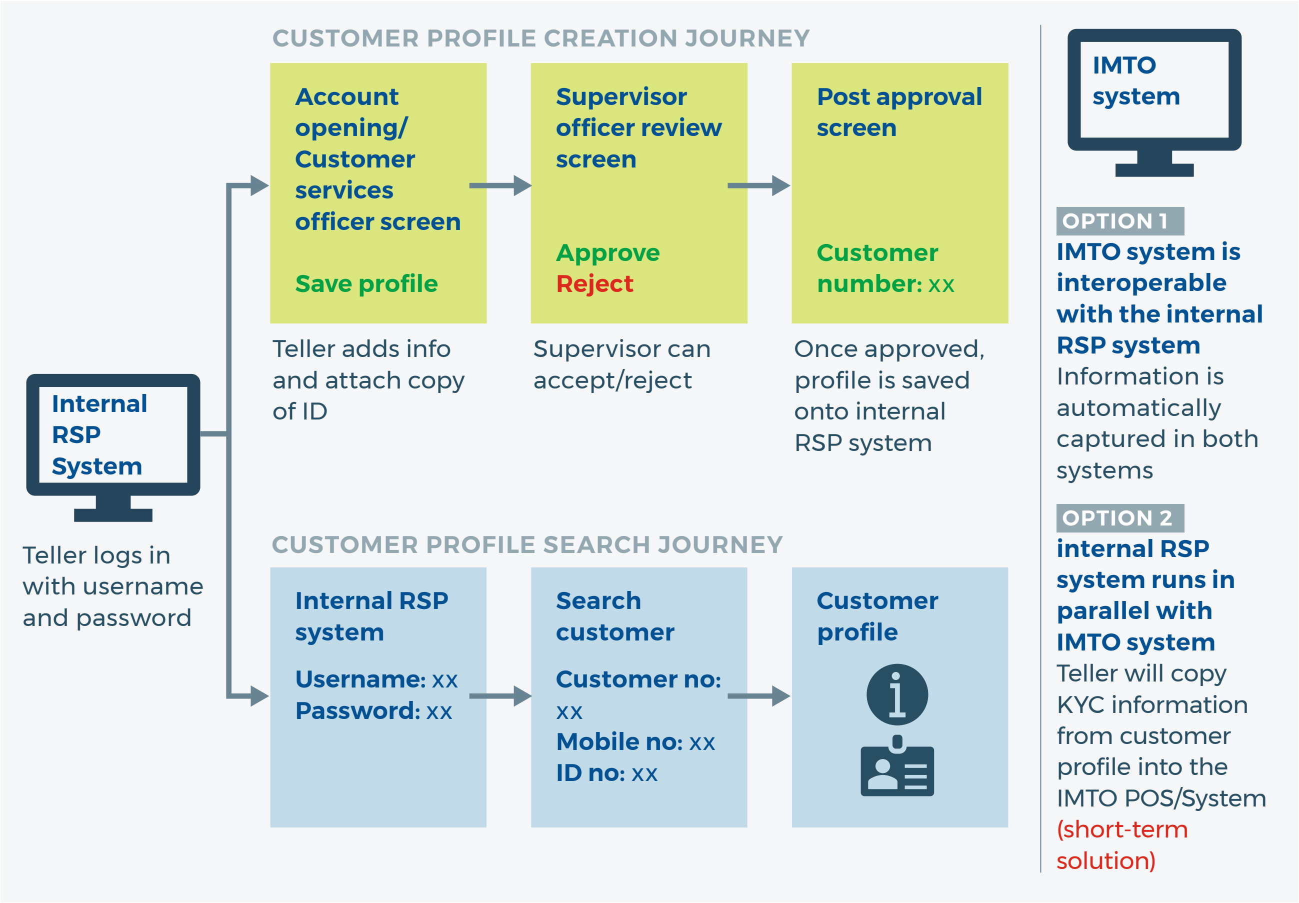
Each profile must have names with a **unique customer number**, such as the customers ID number to make it easy to pull up and link to the customer.[45] This number should remain assigned to the customer for the duration of the relationship with them and will enable you to track their business activity with your institution. From here, in practice, frontline tellers should leverage a built-in interface screen to pull up the customer's profile, using the unique number, to (1) verify the customer's identity; and (b) update their profile using quick and auto-fill enabled fields.

[45] This customer number is not product-specific; thus, a customer can register for more than one product under a customer number (such as a savings account, credit card, remittance account and so forth).

Step 2: Set up the customer interface. Once you have set up the customer profile, introduce the customer interface screen. See figure 3 under the digital ID database to see what this interface could look like – essentially it starts with a log-in page for the frontline teller, followed by a '*search*' page where the frontline teller enters the customer's unique number to pull up their profile, and then the customer's profile page and a log-out option (including an automatic page expiry page). Alternatively, you may wish to align your interface with that of the IMTOs whom you partner with. The teller interface should be easy to pull up and display the remittance customer's information and the copy of their ID to verify that the customer is who they say they are when they return for follow-up transactions.

Figure 4 below shows what the journey looks like from start to finish between your internal system and that of the IMTO. As is evident from the figure below, it is ideal if your system is interoperable with the IMTO's system to avoid duplication of efforts by tellers.

FIGURE 4: **THE TELLER'S JOURNEY FOR USING CUSTOMER PROFILES**



Internal RSP System

Teller logs in with username and password

CUSTOMER PROFILE CREATION JOURNEY

Account opening/ Customer services officer screen

Save profile

Teller adds info and attach copy of ID

Supervisor officer review screen

Approve
Reject

Supervisor can accept/reject

Post approval screen

Customer number: xx

Once approved, profile is saved onto internal RSP system

CUSTOMER PROFILE SEARCH JOURNEY

Internal RSP system

Username: xx
Password: xx

Search customer

Customer no: xx
Mobile no: xx
ID no: xx

Customer profile

IMTO system

OPTION 1

IMTO system is interoperable with the internal RSP system

Information is automatically captured in both systems

OPTION 2

internal RSP system runs in parallel with IMTO system

Teller will copy KYC information from customer profile into the IMTO POS/System (short-term solution)

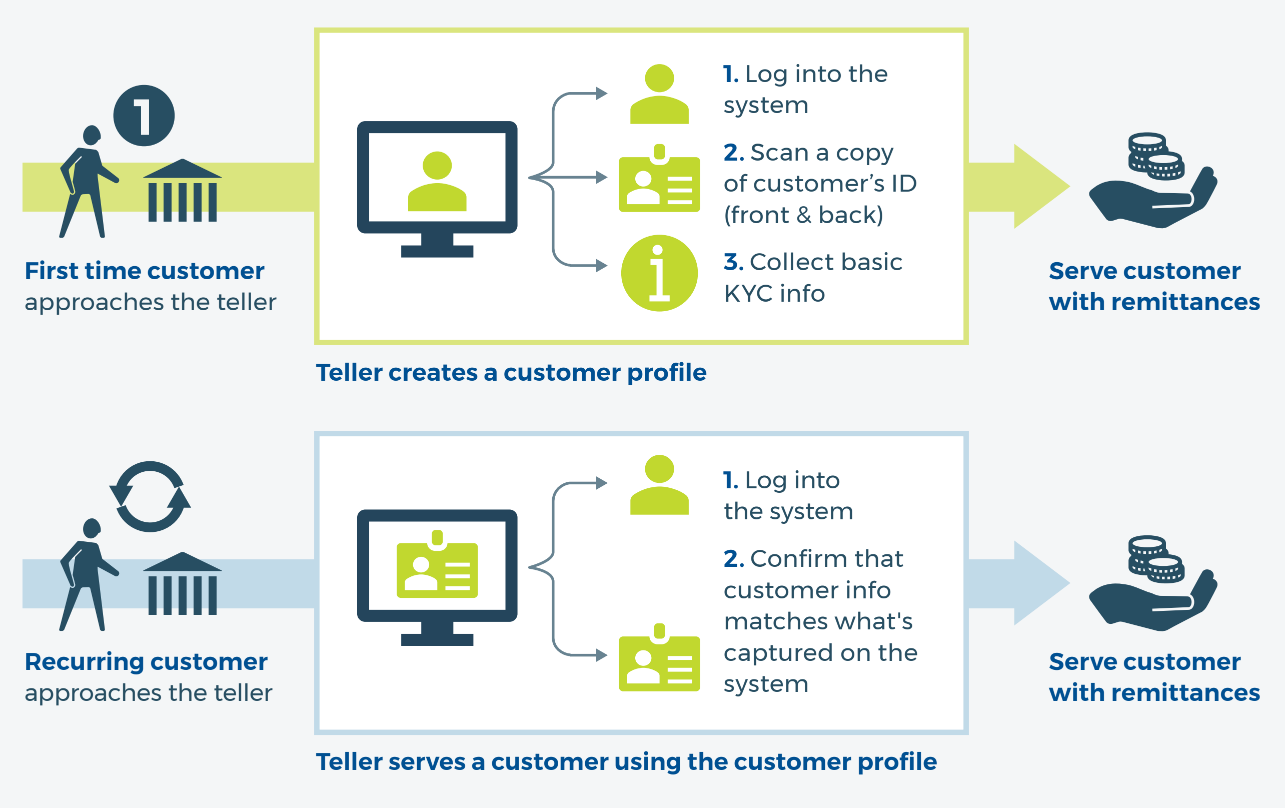
Step 3: Set up appropriate security standards and procedures. For this system to work effectively and efficiently, it needs to be complemented with appropriate security processes and standards. This would include, among others, based on your context:

- Limiting the use of frontline tellers to uploading and viewing customer pages
- Having separate screens for profile creators and supervisors who must verify the profile created
- Limiting the visibility of information by branch to protect customer information between branches
- Restricting login details to company-approved identifiers, e.g. allowing only company-hosted email addresses
- Displaying customer records only once a staff member is logged in and a reference code is added (e.g. ID number or cell phone number)
- Incorporating an audit trail which tracks the time spent when logged in, and who logged into the system at which times
- Introducing an automated time-out after a certain amount of time to limit the risk of unauthorized access to the system
- Introducing ID and document watermarking to prevent identity theft through screen photographs by staff
- Ensuring that only managers can delete and change customer pages and that these pages remain up to date

Step 4: Train frontline staff. After step 3 it is time to start preparing your staff for the imminent changes to their processes. This is done first by training front-line staff members as they must use the updated system and explain the changes to the customers. The best way to do this is to develop a training manual which includes at least the following elements: (a) what the intervention entails; (b) the benefits of the intervention; (c) how to serve remittance sending or receiving customers, respectively; (d) how to create a customer profile; and (e) how tellers can spot fraud or incorrect customer information and what to do when they suspect a customer ID to be fraudulent. These materials can also be used as a way of documenting changes for future staff members. In the training session(s), ideally include branch managers, customer service representatives, front-line tellers and compliance staff and cover the materials included in the training manual. Finally, also include a live demonstration of how to use the system.

Figure 5 below provides an illustrative example of how the database can be used for the remittance context once it is developed and a customer's ID copy has been saved onto the database. Examples like these on relevant process changes would be included in your training manual and live demonstration.

FIGURE 5: THE CUSTOMER JOURNEY WHEN USING CUSTOMER PROFILES


First time customer
approaches the teller
1. Log into the system
2. Scan a copy of customer's ID (front & back)
3. Collect basic KYC info
Teller creates a customer profile
Serve customer with remittances
Recurring customer
approaches the teller
1. Log into the system
2. Confirm that customer info matches what's captured on the system
Teller serves a customer using the customer profile
Serve customer with remittances

First-time remittance-receiving customers will follow the same process as for the digital ID database intervention (section 3.2). The biggest changes under the customer profile intervention occur for returning customers who will not be subject to full KYC and CDD again, as the teller can use the search function in the database, enter the customer's national identity number, and retrieve the digital copy of the customer's ID to verify their identity and proceed with the transaction.

Step 5: After training staff, the next step is to sensitize customers. Customers need to understand the upcoming changes to their customer journey. This can be done by various means, including using various media channels as well as developing posters to place in branches of how the customer journey will change for new and recurring OTC customers and assigning members of staff to explain the new process to customers as they enter. The methods covered under the digital ID database intervention for customer sensitization will also be effective for this intervention.

Step 6: Pilot the intervention. To test how the intervention lands with your stakeholders, it is recommended to launch a pilot test. It is best to launch this pilot in a controlled environment, e.g. in select branches that target a broad range of customers. This step is crucial to ensure that any glitches are ironed out before the intervention is rolled out large-scale across all branches. Table 19 below provides an overview of the suggested activities for a successful pilot, as well as the suggested timelines, to be amended for your context.

TABLE 19: DRAFT PROCESS FOR A CUSTOMER PROFILE INTERVENTION PILOT

Activity	Timeline
Get business and risk department approval for the customer profile	Month 1
Select a branch to test the solution via UAT	Month 1
Arrange a scanner and computer that will be used to test the application	Month 1
Arrange a testing session with your software developers	Month 1
If testing is successful, identify two branches for pilot testing	Month 1
Train two branches for the pilot	Month 2
Pilot test for three months at two branches	Months 3–5
Launch at all branches	Month 5
Collect data for six months after implementation	Months 6–12

Step 7: Roll out the intervention. After ironing out any glitches in the system, you are ready to roll out the intervention to your branches. During implementation, it would be good to determine what the customer and staff feedback is. Based on the feedback, you can identify new opportunities for your organization and determine which aspects require improvement.

KEY LESSONS REGARDING THIS INTERVENTION

LESSON 1 **Ensure that you have the in-house capacity to implement and maintain the intervention.** This includes the necessary system storage space and a staff member trained as a software developer.

LESSON 2 **Conduct troubleshooting throughout the system design process.** Since this intervention is quite technical, frequent check-ins, or “dry runs”, to test new features and feedback sessions with developers are key to ensure that issues are spotted early on.

LESSON 3 **Need for a sufficient timeframe to realise impact.** The customer profile intervention can take significant time to be approved and adopted, as RSPs usually require more time to get internal sign-off (if there are management concerns that such an intervention might create risks of non-compliance). The need for technology and systems-based innovations, and the associated investment in financial and technical resources, also require relatively longer timelines. In addition, benefits such as significant reduction in fraud, decreased cost of compliance, and enhanced customer experience will only materialise once the intervention has reached scale.

LESSON 4 **Account for challenges in customer uptake.** Customers may be slow to take to this intervention because it will take longer on their first time to receive/send remittances as the profiles are set up. The benefits for the customer are only realised once the customer comes back (recurring) and for the business when sufficient OTC customers have set up profiles.

Table 20 below provides an overview of the dos and don’ts to bear in mind when deciding to implement this intervention.

TABLE 20: DOs AND DON'Ts OF THE REMITTANCE CUSTOMER PROFILE

✓ Dos	✗ Don'ts
Explore how the customer profile can be used in other innovative ways, for example: leveraging the data drawn from the customer profiles to make marketing decisions (based on a better understanding of your client base) and even to consider new products	Don't let the customer profile data go to waste, this system needs to become a living entity that feeds into your strategy. Be sure to collect and analyse customer data and draw synthesized insights for your business unit
Consult the regulations and/or regulator on recordkeeping and data privacy requirements when saving an ID copy on your system	Don't forget about data and privacy laws

MEASURING YOUR SUCCESS

Developing key indicators to measure success. The next step before starting with the implementation of this intervention, is to determine what your key indicators of success are. This will also be based on what you want to achieve with the intervention (for example, reducing fraud). Key indicators include:[46]

- Number of customer profiles created for OTC customers
- Increase in the number of remittance customers served using the customer profiles
- Amount of time spent per transaction
- Number of transactions per profile
- Number of cross-selling opportunities or successful cross-selling services (e.g. savings account, e-wallets, credit options) based on customer profile and transaction history47
- Number of fraud cases reported for OTC transactions (compared between piloted and non-piloted branches)
- Number of fraud notifications (before and after implementation of the intervention)
- Number of customers who lost money due to fraudsters
- Change in marketing[48] and securing recurring revenue costs

When taken together, the enhanced efficiency indicated by the above indicators will assist in calculating the overall decreased cost of compliance.

[46] Note: where possible, these indicators should include the SDGs, as when people are engaged in the economy, they can become more prosperous and have increased activity which can benefit your organisation. Each of the data indicators should be segmented by e.g. urban/rural, age, gender, etc. to gain a better understanding of your customer base, to expand reach and to ensure better product development and -offerings.

[47] For examples on effective cross-selling opportunities, you can refer to the case studies in Cenfri, UNCDF & FinMark Trust's Making Access Possible (MAP) reports in Nepal and Cambodia.

[48] Each customer profile brings additional marketing opportunities, which cuts down on marketing costs as it directs those costs to more viable leads.

Collecting data and assessing the impact. To get an accurate measure, you should start data collection before the intervention is launched. To do this you can either plan by collecting data pre-implementation, or you can rely on historical data per indicator if such data is available. It is recommended to use data six months before the intervention is launched and compare it to a six-month period where the intervention is active – to account for seasonal changes. For example, if you plan to implement the intervention in March of Year 2, you will need to collect data for March–August of Year 1, and then again for March–August of Year 2. To analyse this data, use a relevant data analysis tool, such as Excel. As part of the analysis, conduct calculations like determining the growth in the number of customer profiles created in the system. It is advised that these calculations be done both on a month-to-month basis, as well as on a year-on-year basis to show the growth after implementation, as well as the comparison between pre- and post-implementation. It is recommended that you track these indicators even after the pilot and then report these figures to management on a bi-annual basis.

3.4 Replacing manual forms with printed receipts

INTERVENTION CHECKPOINT

Manual processes are inconvenient and exclusionary for less literate customers. When it comes to sending and receiving remittances, many institutions in less mature market segments still ask their OTC customers to complete a manual money transfer form. However, people who are semi-literate, or not financially literate, struggle with completing manual money transfer forms independently. Given that tellers are often not permitted to help customers, due to risk, many are reliant on bringing friends or family with them to help them with this process. This ultimately acts as a barrier to accessing remittances. This same barrier is also a challenge for people who do not speak the language that the form is in. In this digital age, such forms are an inconvenience for customers.

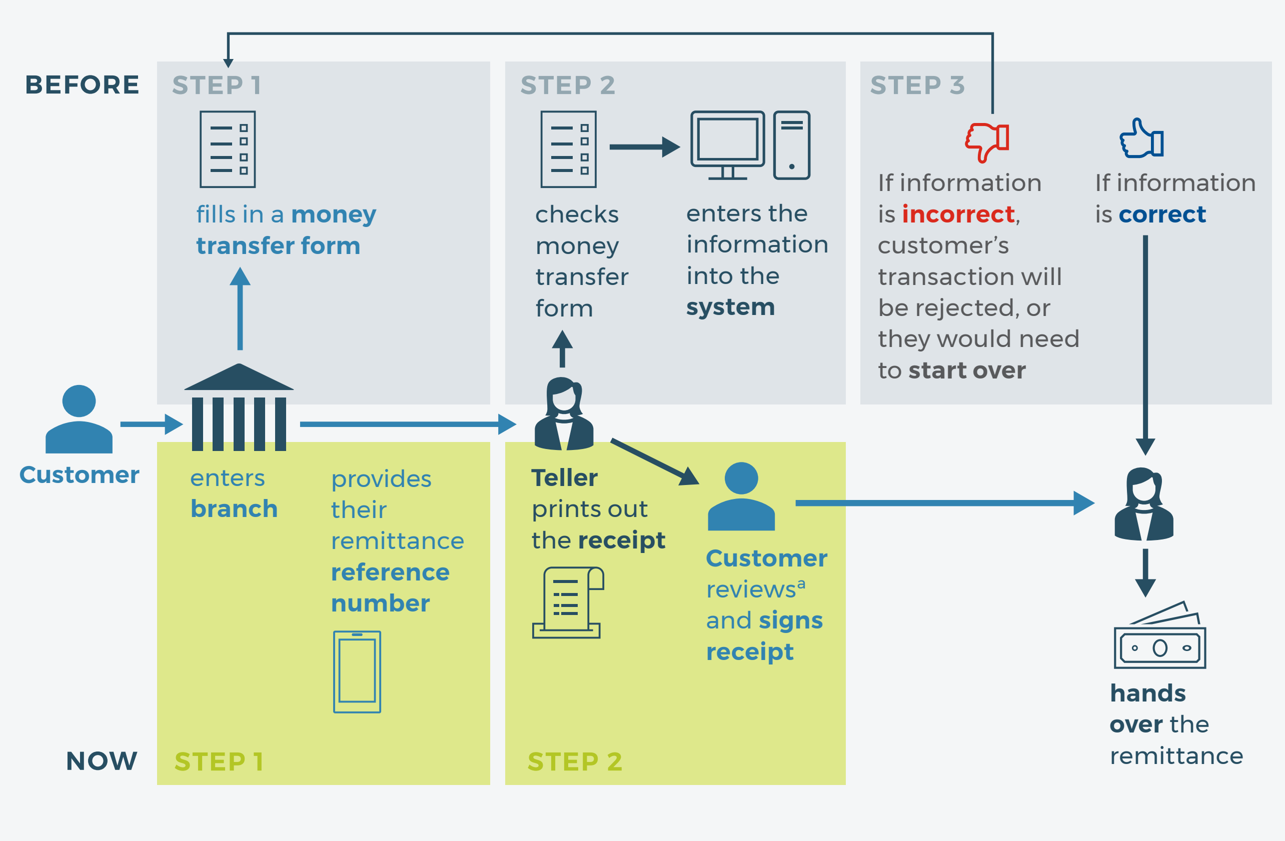
Manual processes may result in lost customers and added costs. Research conducted during the RAI programme suggests that it takes approximately 24 minutes for customers to complete the form and receive their remittances, while it takes on average 5–10 minutes longer to serve remittance-sending customers, which negatively impacts their overall experience.[49] In addition, if forms are not accurately completed, the RSP must often reject the transaction to mitigate risk related to fraud. This process is also costly for RSPs as they must print money transfer forms for use in their branches and their tellers spend unnecessary time entering this information manually into their digital system. This is time that could have been better spent serving more customers. Digitalising the remittance sending and receiving process has the potential to address the challenges for both customers and the RSP.

[49] Source: data collected during the IFAD RAI programme, conducted from 2021–2023

The printed receipt is a simple solution for digitalising the remittance sending and receiving process. Despite asking customers to complete manual forms to collect remittances, some RSPs already have the information that they need on their systems. This is usually found in their IMTO files, and it includes information needed for CDD such as name, address, date of birth, ID number and purpose of transaction. There is thus an opportunity to leverage this existing information instead of duplicating efforts by asking customers to re-add it on a manual form, and then ask tellers to re-enter into their systems. An elegant solution is to print out the information RSPs have in the form of a printed receipt and ask the customer to review and confirm it before serving them with their remittances. The intervention therefore entails removing manual money transfer forms and switching to printed receipts to reduce the chance of error and cut down on duplicate processes.

Figure 6 below provides an overview of the customer journey when using printed receipts.

FIGURE 6: **CUSTOMER JOURNEY WHEN USING PRINTED RECEIPTS**


BEFORE
STEP 1
fills in a money transfer form
STEP 2
checks money transfer form
enters the information into the system
STEP 3
If information is incorrect, customer's transaction will be rejected, or they would need to start over
If information is correct
Customer
enters branch
provides their remittance reference number
Teller prints out the receipt
Customer reviews[a] and signs receipt
hands over the remittance
NOW
STEP 1
STEP 2

Note: [a] The teller can also assist the customer in understanding and reviewing the information

Before you dive in, weigh up the costs and benefits. To determine whether this intervention is worthwhile, it is important to compare the costs and benefits associated with implementing the intervention. The table below provides a guide for how you can think about estimating the costs and benefits of the intervention within your context.

TABLE 21: COSTS AND BENEFITS OF THE INTERVENTION TO REPLACE MANUAL FORMS

Benefits
• **Cutting down process duplication** by replacing manual money transfer forms • **Improved customer retention** due to improved service and fewer rejected transactions due to incorrectly filled-in forms • **Growth in remittance transactions.** An RSP under the RAI programme found it can equate to over 40 per cent increased number of transactions • **Increased number of returning customers**, with one RSP under the RAI programme indicating an expected additional 1700 returning customers per year • **Reduced record storage** of paper-based forms for the institution by having all details of remittance transactions in digital form • **Improved turn-around time** by cutting out the additional steps, saving approximately 10 minutes per transaction (based on findings from the RAI) • **Reduced chances of error** in the remittance process by removing the need for frontline tellers to assist customers in filling in money transfer forms and decreasing risk as all the fields on the receipt are automated and pulled directly from the system • **Improved customer experience** through shorter waiting times and modernized processes thereby enhancing business efficiency • **Identification of new opportunities** by using the learnings from digitising this process and applying it to other processes or products, like rolling out the intervention to outbound remittances as well[50]
Costs
• **Internal time and capacity** needed to assess IMTO files and data requirements, and manage the project (including stakeholder coordination, piloting etc.). This includes IT or software development team time spent in ensuring that the printed receipts hold the same information as the manual forms • **System-change related costs** if the existing system does not have the functionality to automate the receipts or integrate with the IMTO systems

Getting ready – key considerations when implementing this intervention

- **Time:** roughly five months (without delays) and an average of 12 months (with moderate delays) from design to implementation. This is estimated based on the assumption that you will have managerial buy-in, that you are using a non-IMTO linked product or if so that IMTOs have already agreed to implement this intervention on their platforms.
- **Capacity:** leveraging the internal technology team or getting a software developer on board to design and implement any systems changes, as well as ensuring that staff are trained on the changes required in their processes.
- **Key dependencies:** alignment with IMTOs to ensure that they are aware of the intervention and how it can change documentation requirements, ensuring that there is system interoperability with that of the IMTOs, and overcoming inertia within the organization to do away with paper-based forms.
- **Regulatory considerations:** consider the regulatory assessment for your country, specifically drawing on AML/CFT acts, laws, regulations, directives and guidelines. Key things to consider includes recordkeeping requirements.

[50] For example, under the RAI, insights showed a need for further introducing digital solutions in branches, i.e. automating other service offerings much like the printed receipt. This includes setting up self-service stations to further reduce pressure on tellers.

What success can look like – testimonial from the RAI:

Ecobank Ghana implemented the printed receipts intervention. So far, they have shared the following feedback regarding the intervention:

- "Today **all customers feel comfortable** using our flagship remittance product Rapid Transfer through the system printed receipts intervention at our branches."
- "Customers are not intimidated and as such people of all income classes **or different literacy levels are able to use the service**."
- "Another area of benefit is the **reduced process flow** for remittance tellers thus a better experience for the customer."
- "We have [also] seen a **consistent growth in transactions**."

Implementation advice from this financial inclusion champion for others interested in implementing this intervention: Obtain buy-in from senior management and assign resources to the project very early in the process. Also, examine the existing technology that will be impacted or utilized.

Ecobank is a pan-African remittance service provider, with banking operations in 33 African countries, including Ghana. It is the leading independent regional banking group in West Africa and Central Africa and serves both wholesale and retail customers.

A STEP-BY-STEP GUIDE TO IMPLEMENTATION

Step 1: Identify the fields not represented on the printed receipt. In your customer-facing remittance sending/receiving process, there are three key components: (1) the manual receipt form that customers complete by hand; (2) the IMTO file with data points in your system; and (3) an existing printed system receipt that customers sign when sending/receiving remittances as a proof of payment. This essentially shows that there is information that the teller needs to add to the system printed receipt from the manual form to ensure it is complete and to meet the IMTO's compliance checks.

This intervention aims to align the information between the IMTO file and the printed receipt to make the manual form redundant. Therefore, in defining what needs to be on the final printed system receipt, you need to compare what is currently required on the manual form, what is on the IMTO file and desirable to be on the printed receipt and any differences to be considered.

The first step is to compare the information you currently have on your IMTO remittance file to the information you request on your money transfer form (which is usually the same as your existing system-printed receipt). When comparing, you need to highlight what information exists on the IMTO remittance file that is not on the money transfer form (or vice-versa).

Step 2: Add missing fields to the printed receipt. Table 22 below shows an example case with the typical information points that you can find on the IMTO file, compared to what is usually captured on the printed system receipt. The highlighted rows, in green, indicate where there is a field difference between the two sources. These fields are what will need to be added to the printed receipt from the IMTO file to ensure that your printed receipt has all the information required. In the example case, only the "occupation" and "purpose of transaction" fields would need to be added to the receipts.

TABLE 22: **EXAMPLE COMPARING THE IMTO FILE AND THE SYSTEM RECEIPT**

Customer Information		Available on the IMTO file	Printed on System Receipt
		(Yes/No)	(Yes/No)
Recipient			
1	Full name	Yes	Yes
2	Date of birth	Yes	Yes
3	Address	Yes	Yes
4	ID number	Yes	Yes
5	ID Type	Yes	Yes
6	ID issuance date	No	No
7	ID expiry date	No	No
8	ID issuance country	No	No
9	Father's/husband's name	No	No
10	Phone number	Yes	Yes
11	Occupation	Yes	No
12	Purpose of transaction	Yes	No
13	Relationship to sender	No	No
14	Account number	Yes	Yes
Sender			
1	Full name	Yes	Yes
2	Payment originating country	Yes	Yes
3	Amount	Yes	Yes

This will allow for a more streamlined process, which is one of the main goals of the intervention. If you already have a printed system receipts system in place, you will add additional information fields from your system to the receipt or replicate the information fields already housed on your system onto the printed receipt. This change will allow customers to collect remittances without needing to complete a form as the receipt automatically prints out all their relevant information.

Step 3: Train your staff. The next step is to train your staff. This is done first by There is a requirement for manual data to be input by the teller, that is not a system receipt, that is a manual return to the IMTO. We specify what information needs to be collected manually or through the system to be entered on the IMTO receipt to prove the RSP paid the right person. So, we need to compare what the IMTO requires, what we can source from the IMTO file and what we can source elsewhere on the system or through any eKYC, etc. and then place those on the SGR. The SGR is then signed as the IMTO receipt and returned to them. training front-line staff members. The best way to do this is to develop a training manual which includes at least the following elements: (a) what the intervention entails; (b) the benefits of the intervention; (c) changes to the remittance-receiving process; (d) procedures for staff to follow; and (e) how to promote internal awareness and knowledge sharing. These materials can also be used as a way of documenting changes for future staff members. In the training session(s), ideally include branch managers, customer service representatives, front-line tellers and compliance staff and cover the materials included in the training manual. Finally, also include information on how the customer journey has changed as shown in figure 6 above.

Step 4: Sensitize customers to the new process. To encourage uptake of the intervention, it is also key to roll out targeted marketing campaigns to the existing customer base (e.g. via SMS blasts and brochures) to inform them of the system changes. Ideally, this would be done more than one month before the intervention is launched and continued for six months after the intervention has been implemented to help customers adjust. It is also advised to assign a customer service representative to assist clients with the new process in the first few weeks after implementation.

Step 5: Pilot the intervention. As with the other interventions, it is advised to launch a pilot test to test how the intervention lands with customers and staff members. This step is crucial to ensure that any glitches are ironed out before the intervention is rolled out large-scale across all branches. To pilot, you could select two to three key branches in different regions. The customer base in these selected branches needs to have a good combination of rural and urban customers, as well as men and women to ensure that you get a good grasp of how the intervention will work with various aspects of your customer base. Next, start with the training and sensitization of the intervention, as covered in Step 4, for one month. Thereafter, roll out the pilot process for approximately 6 months (with delays) and three months (without delays). While rolling out the pilot, ensure that you follow the data collection processes outlined in section 3.4.4 below to measure impact and correct challenges. Throughout this process, remain aware of challenges that may arise and ensure that they are dealt with promptly before the intervention is rolled out to your branches. Examples of challenges include a lack of internal buy-in, customers still requesting to fill in manual forms, network connectivity in branches and system capabilities.

Step 6: Roll out the intervention. After ironing out any glitches in the system, you are ready to roll out the intervention to your branches. It is advised to share the data on the success of the pilot with your management team to obtain buy-in so that this intervention can be rolled out to other branches.

TIP The intervention will be most effective if it is implemented as a required change for all branches across the institution. Therefore, managerial buy-in early on and throughout the design and implementation of the intervention is crucial.

KEY LESSONS REGARDING THIS INTERVENTION

LESSON 1 Leverage existing IMTO information. This intervention will be much easier to implement if you already have most of the information on your IMTO files.

LESSON 2 Start with your own product, then move to partner products. Implement this intervention with your internal product first before rolling it out to other products you offer via IMTO partners. This will allow you to streamline the decision-making process and roll the intervention out, thereby testing it to iron out any challenges and collect evidence of its success. The latter can then be used to inform your business case when approaching IMTO partners.

Table 23 below provides an overview of the dos and don'ts to bear in mind when deciding to implement this intervention.

TABLE 23: **DOs AND DON'Ts OF THE AGENT EXPANSION AND MANAGEMENT INTERVENTION**

✓ Dos	✗ Don'ts
Start implementation with your internal product first	Don't take on too much by implementing this intervention across all your products or platforms as it may cause complications and delays
Start data collection a year before the planned roll-out of the intervention (accounts for seasonality) or leverage historical data if available	Don't start data collection only after rolling out the intervention as this will limit your ability to assess its true impact
Assign dedicated team member(s) as resources to the project	Don't implement this intervention without a clear project manager who has access to the necessary data sources, departments and decision makers
Ensure that you sensitize your stakeholders on the intervention from the beginning, to enhance buy-in	Don't assume that your top management, staff and customers will be automatically bought in to the changes. A lack of buy-in has the potential to negatively impact the roll out and uptake of the intervention

MEASURING YOUR SUCCESS

How to measure intervention success by comparing impact to baseline data. Before launching this intervention, you need to determine what your key indicators of success are. Key indicators include:[51]Number of customers served using the printed receipt

- Number of rejected transactions (number of OTC remittance transactions rejected due to incomplete or inaccurate filling in of remittance forms)
- Average time spent serving OTC customers: (1) average time spent on serving customers with the money transfer form, versus (2) average time spent on serving customers using the printed receipt. Do this for (a) remittances being sent and (b) remittances being received
- Number of reported fraud cases in branches with and without the printed receipt
- Change (reduction) in marketing[52] and securing recurring revenue costs
- Change (reduction) in losses due to customers who have been turned away from receiving their remittances

When taken together, the enhanced efficiency indicated by the above indicators will assist in calculating the overall decreased cost of compliance.

Note: These indicators will be based on the challenges that you identified during the planning stages of this intervention, such as customers being turned away from receiving remittances due to incomplete or inaccurate money transfer forms. To get an accurate measure, you will need to start data collection before the intervention is launched. To do this you can either plan by collecting data pre-implementation, or you can rely on historical data per indicator if such data is available.

TIP After you start recording success from rolling out the intervention for your remittance receiving product, consider using it for other use cases such as sending remittances or cash withdrawals.

[51] Note: where possible, these indicators should include the SDGs, as when people are engaged in the economy, they can become more prosperous and have increased activity which can benefit your organisation. Each of the data indicators should be segmented by e.g. urban/rural, age, gender, etc. to gain a better understanding of your customer base, to expand reach and to ensure better product development and -offerings.

[52] Each customer profile brings additional marketing opportunities, which cuts down on marketing costs as it directs those costs to more viable leads.

3.5 Agent expansion and management

INTERVENTION CHECKPOINT

A new take on onboarding and managing agents. This intervention entails re-assessing the risks related to an RSP's remittance agent network[53] and amending the risk-mitigating processes and onboarding processes accordingly.

Need for expanding RSP presence and business while building trust. Institutions with customer ties in rural areas often experience the challenge that customers struggle to access their remittances due to a lack of physical RSP touchpoints in their area. This requires customers to travel to other areas where agents are located, which can be inconvenient and costly. This can make customers less willing to use the RSP's services and result in an RSP losing customers. Thus, there is a need for increased agent presence in these areas. However, such agents should be trustworthy and welcomed by the locals in these areas. Trust may have been eroded in certain communities due to improper conduct by poorly trained or fraudulent agents, or by agents not having the right amount of liquidity to pay out remittances or by deceiving customers who are illiterate or semi-literate. If customers perceive agents as untrustworthy, the word will travel quickly throughout the community.

RSPs often have few agents due to various reasons, including the fact that prospective agents cannot meet the requirements imposed to qualify as agents. Since agents are representatives of the RSP, regulation often requires that the RSP collects specific information from prospective agents to ensure that (a) they are who they say they are, (b) they are not involved in illegitimate activities and (c) they do not pose a significant risk to the RSP. Generally, RSPs impose more stringent requirements on agents than required by regulation due to a lack of understanding of agent risk or risk aversion.

Weigh up the costs and benefits. To determine whether this intervention is worthwhile, it is important to start by comparing the costs and benefits associated with implementing the intervention. The table below provides a guide for how you can think about estimating the costs and benefits of the intervention within your context.

[53] What is a remittance agent network? A remittance agent network is comprised of independent, small-scale dealers and other shops, or can be part of an existing distribution network like post offices or retail chains. Depending on current laws and regulations, agents can frequently carry out simple financial operations on behalf of banks, including withdrawals, deposits, money transfers, and payments (CGAP, n.d.).

TABLE 24: COSTS AND BENEFITS OF THE AGENT ONBOARDING INTERVENTION

Benefits
Expanding the agent network by reducing unnecessary requirements that inhibit agent onboarding. **Enhancing risk management** for agents by developing a robust agent risk assessment and implementing proportionate risk controls **Identifying new opportunities** by outlining additional ways agents can support your business expansion (e.g. value-added services) **Onboarding more customers** as seen under the RAI programme where a newly onboarded agent could serve an additional 500 customers.
Costs
RSP compliance team time spent in developing a new customer onboarding policy. **Costs related to monitoring agents and** managing a helpline for agents. **Compliance staff time** to conduct an agent risk assessment. **Costs related to doing qualitative data collection** (e.g. field research) to determine agents 'needs and whether the new process meets their needs. Time and resources associated with **action plan, implementation and follow up**

Getting ready – key considerations when implementing this intervention

- **Time:** between approximately six months (without delays) and an average of eight months (with moderate delays) to fully implement the intervention. This is estimated based on the assumption that you will have managerial buy-in, and that you already received approval to make the process changes.
- **Capacity:** regulatory, cultural and risk experts who understand your local context and who would be able to provide guidance on how process changes should take place.
- **Key dependencies:** the ability for the organization to make process changes and the organizational drive needed to recruit more agents.
- **Regulatory considerations:** consider the regulatory assessment for your country, specifically drawing on AML/CFT laws and relevant circulars. Key things to consider includes documentation requirements for agents, how to manage risks when working with agents, etc.

What success can look like – testimonial from the RAI

Wizall Money implemented the agent expansion intervention. According to the Wizall Money implementation team, this intervention has reinforced their commitment to their most vulnerable beneficiaries and provided them with valuable strategic directions to improve their long-term social impact.

- "The intervention provided a valuable external perspective on our operations and practices, which helped us **identify opportunities for improvement** and strengthen our internal processes."
- "… the intervention allowed us to **better understand the specific needs** of these populations and **develop tailored solutions** to serve them more effectively and inclusively".
- "Furthermore, the strategic recommendations made helped us **adjust our policies and programmes to better meet the challenges** faced by low-income and rural households."

Implementation advice from this financial inclusion champion for others interested in implementing this intervention: Conduct an in-depth analysis of initial needs and prioritize transparent and open communication between stakeholders to promote a collaborative working environment.

Wizall is a remittance service provider in Senegal, which was launched in 2015. They offer businesses, non-government organizations and governments an innovative mobile money services for their payments (e.g. remittances) and collections (e.g. bills). Their services are currently available in Senegal, Mali, Burkina Faso and the Ivory Coast.

A STEP-BY-STEP GUIDE TO IMPLEMENTATION

Step 1: Understand the current process and collect data. The first step along the journey to implement this innovation is to understand what your organization's current agent onboarding process looks like, including its KYC and CDD policies and procedures and the implementation journey in practice. This involves looking at the documentation requirements and how long it usually takes to onboard an agent. During this step, you can also look at the most pressing issues that arise when onboarding new agents. Qualitative interviews with agents and with the individuals in your organization who are responsible for onboarding them, as well as recent complaints raised by agents, are valuable sources of information. This should be accompanied by data collection to determine the status quo before the intervention is implemented.

TIP A good point to pause on here is to determine whether prospective agents know which documents they require so that they can be onboarded and whether they know how to go about getting these documents.

Step 2: Map your requirements to those required by regulation. Next, it is important to consider your jurisdiction/regulator's agent documentation requirements and to compare what is required in regulation to the requirements your organization is imposing. This is a great opportunity to determine where you are applying more stringent requirements than required by regulation, and to identify which methodology and technology you can employ to make the agent onboarding experience more accessible, while effectively managing risks. This also provides the opportunity to identify potential areas for innovation where the regulation is not clear on how information should be gathered (e.g. format to prove address).

Step 3: Conduct a risk assessment on your agent business. After identifying where your organization can improve and innovate, your next step will be to assess the risks related to your agent business. To do this, navigate to table 34 of the Appendix accompanying chapter 3.5, to the agent onboarding section. Thereafter, add the risks posed by agents, your mitigation strategies and the weighting associated with each risk.

Step 4: Consider alternative requirements and amend your onboarding process. Based on the outcomes of your risk assessment in Step 3, you will know which risks related to agents need to be mitigated by documentation requirements and due diligence measures. If you cannot remove certain requirements, you may be able to consider alternatives, such as using proxy identifiers.

Using alternative documentation requirements

- To prove that an agent is legitimate, a business registration form is often required. However, many agents may struggle with this requirement due to a lack of access to the required documentation.
- In these situations, you can consider implementing an alternative option like designing a form where another trusted entity in the community can vouch for the agent's legitimacy.

The next part of this step is to amend the onboarding process. This entails firstly amending your agent onboarding policy to be more risk-based, e.g. only requiring necessary documents that mitigate risks and moving away from over-compliance. Table 25 below provides an indicative example of the documentation requirements before and after the intervention.

TABLE 25: DOCUMENTATION REQUIREMENTS BEFORE AND AFTER THE AGENT EXPANSION INTERVENTION

Requirements pre-intervention	Requirements post-intervention
Provide the following documents to be eligible for onboarding as an agent: • Proof of business registration • The contract signed by both parties. • The agent's ID • A recent proof of address dating back at least six months	Agents are allowed to use an affidavit form to be used as a substitute for the proof of registration. The rest of the documentation requirements remain in place.

Step 5: Onboard pilot agents. Once you have changed the onboarding process, conduct a pilot on a sample of new agents who are applying to be onboarded. This pilot could run for three months and be conducted in a controlled environment, e.g. only in 2–3 rural areas, or where you found the challenge to be the most pressing. This is then accompanied by data collection on the change in customer transactions in that area, as well as small customer surveys and interviews with the agents to determine whether the intervention is having the desired outcome.

> **TIP** If you find the intervention successful with the changes in documentation requirements, a future opportunity is to explore how you can support potential agents in getting business registration instead of using a form where others in the community must vouch for their legitimacy and proof of address.

Step 6: Roll out the intervention. After completing the pilot and ironing out any issues that may arise, you will be ready to roll out the intervention to your broader network. During this step, you may need to invest in more staff who will be able to take prospective agents through the onboarding process and requirements and continue marketing the new locations where agents will be present to your target market.

Step 7: Market agent expansion to your customer base. A key activity to ensure the success of the implementation journey is to raise awareness of the expansion of your agent network among existing and prospective customers. This will create interest in your service among prospective customers and signal convenience to your existing customer base in that area who will now no longer have to travel very far to process a remittance transaction.

KEY LESSONS REGARDING THIS INTERVENTION

LESSON 1 This intervention as an ongoing process: you can do initial due diligence on agents, but you should also do checks and balances over time. Indicators to look for includes the flow, the throughput, the quality of documents, and the identifiers coming in via the agents.

If you have very accessible agent onboarding processes, then you need to be quite cautious with your monitoring and vet a lot of the information coming through to identify bad actors. The lighter you go on initial agent onboarding requirements, the tighter you must be conducting ongoing due diligence. It is recommended that you also do risk assessment for agents continuously.

LESSON 2 Set aside enough time to do qualitative research with agents in rural areas. They are often difficult to reach, but their insights are crucial to determine whether the intervention was successful – and could even spark ideas for further innovation, based on their practical knowledge of their customer base's needs.

For example, to get on-the-ground feedback on how the changes are faring in practice, you can conduct quick interviews with agents in the field to determine whether the onboarding process is now clearer and less onerous. Depending on the alternative documents that you impose, you can also ask whether the changes allowed them to be onboarded more easily.

Table 26 below provides an overview of the dos and don'ts to bear in mind when deciding to implement this intervention.

TABLE 26: DOs AND DON'Ts OF THE AGENT EXPANSION INTERVENTION

✓ Dos	✗ Don'ts
Conduct a thorough risk assessment to inform your new process.	Don't remove requirements without conducting a risk assessment.
Use data to indicate where the biggest need for agents is (e.g. which locations).	Don't attempt this intervention without using data.
Ensure that your strategic priorities include expanding your rural agent network if you wish to implement this intervention.	Don't choose this intervention if it is not a strategic priority for you.
Ensure that ownership and accountability of the intervention are clear, and that processes are properly documented within the organization.	Don't fall victim to the key man risk[54] by only having one person owning the intervention.
Meticulously document steps to facilitate training new team members and agents.	Don't assume your internal staff will know about the process changes.
Strategize around change management to sensitize rural communities on using agents for remittances.	Don't assume that rural communities will adopt change quickly.
Assign a staff member to explain what the requirements, rights and responsibilities for agents are	Don't leave potential agents in the dark.

[54] Key Person Risk refers to the potential risk arising when a substantial amount of organisational knowledge, visibility, status, or performance is heavily dependent on a single individual (Open Risk Manual, n.d.).

MEASURING YOUR SUCCESS

Measure intervention success by comparing impact to baseline data. This intervention will benefit from qualitative data collection to better understand the core issues facing the customer base and prospective agents before embarking on the intervention. A few questions to ask during the qualitative data collection process includes:

- How many prospective agents did you have to turn away/reject due to lack of documentation?
- How many customer complaints did you receive due to inconveniently located remittance-access points?
- How do the pre-intervention onboarding requirements compare to the requirements of your competitors?
- Are prospective agents incentivized to become an agent of your organization?

Once you understand what the key challenges are that are facing your customer base and agents, you need to determine what your key indicators of success are. Key indicators include:[55]

- Number of new agents onboarded.
- Number of new locations reached.
- Time taken to complete agent onboarding (ideally, measured against how long it usually takes to onboard agents before the implementation of the intervention).
- Number of fraudulent transactions reported (before and after the intervention was implemented).
- Number of system abuse attempts or incidents (before and after the intervention was implemented).
- Number of customers each agent could serve – in the near-term and the medium-term/over time.

When taken together, the enhanced efficiency indicated by the above indicators will assist in calculating the overall decreased cost of compliance.

These indicators will be based on the challenges that you identified during the planning stages of this intervention. To get an accurate measure, you will need to start data collection before the intervention is launched. To do this you can either plan by collecting data pre-implementation, or you can rely on historical data per indicator if such data is available.

[55] Note: where possible, these indicators should include the SDGs, as when people are engaged in the economy, they can become more prosperous and have increased activity which can benefit your organisation. Each of the data indicators should be segmented by e.g. urban/rural, age, gender, etc. to gain a better understanding of your customer base.

4

Conclusion

This toolkit paves the road to enhancing remittance access and growth:

- **It provides regulators and RSPs with practical guidance** on how to (1) assess and appreciate national regulatory environments and delineate relevant compliance-based regulatory parameters; (2) analyse their own business realities, highlighting key risks and opportunities for innovation; and (3) plan, implement and measure innovative interventions to address KYC and CDD barriers to remittances.

- **It is widely applicable in the African context.** The intervention approach, and the five detailed interventions delineated in this toolkit have been tried and tested with select RSPs in seven African markets. Each jurisdiction has its own regulatory and contextual nuances that must be appreciated to ensure that innovative interventions aimed at enhancing remittance access have the desired impact. In applying this toolkit, regulators and RSPs must take account of their unique contexts and use the tools to amend the intervention journey and the provided interventions to serve their own needs and realities.

- **It equips regulators and RSPs to enable financial inclusion and capitalize on innovation.** The practical guidance provided in this toolkit enables regulators and RSPs to enhance remittance access whilst strengthening risk mitigation measures, thereby unlocking wider, systemic change.[56] When implemented correctly, the interventions included in this toolkit also hold a myriad of benefits for RSPs.[57]

- **It paves the way for discussions on innovations in risk management.** The toolkit also helps RSPs to continually improve their risk assessment and management practices. The guidance provided aims to reshape industry players' thinking around risk management, away from a tick-box

[56] Including decreasing the cost of remittances, enhancing access to broader financial services, supporting livelihoods, and poverty alleviation.

[57] Most notably, the interventions enable operational and compliance cost reduction and enhance access to remittances thereby increasing the number of customers who can be served and, in turn, productivity.

or compliance approach and toward practices that truly mitigate risks and improve daily operations and customer experience. This can steer RSPs towards greater resilience and inclusive financial integrity, ensuring their efforts in risk management are both effective and adaptive.

Integration of the toolkit learnings and best practices into existing and planned practices and processes on an ongoing basis is key for success. For stakeholders to get maximum benefit from the toolkit and its interventions, it is essential for them to **integrate the guidance provided in this toolkit into existing practices and processes.**

- **RSPs** should integrate this toolkit into their business procedures and leverage it on an ongoing basis when updating risk assessments or when considering new KYC and CDD related innovations.
- **Regulators** should integrate the contents of the toolkit into their practices to: (1) react and respond to market realities, for example, course correcting, enhancing further innovation and addressing existing and emerging risks; and (2) proactively shape the market by setting new standards for new market entrants. One way could be to share this toolkit and relevant sections with any new RSP registering in their jurisdiction.

The guidance provided by this toolkit should catalyse sustainable, resilient and innovative growth in the remittance market, thereby empowering livelihoods and propelling national development objectives.

5 Appendix

5.1 Deep dive 1: Leveraging remittances to bolster growth in Africa

Remittances play a crucial role in the lives of millions worldwide. According to IFAD (2023), approximately 800 million people receive remittances from 200 million migrants every year. A closer look shows that remittances are a lifeline for one in every eight people globally: providing access to food, healthcare and education. They also enable economic agency by allowing receivers to grow small businesses and even access credit, particularly in less developed economies (Piras, 2023). For example, 44 per cent of Senegalese households that receive international remittances, reinvest in their business and develop strategies to manage agricultural risks (IFAD, 2020). This substantial support has a powerful spillover effect; the World Bank highlights a recent study that found that a 10 per cent increase in remittance is associated with a 0.66 per cent permanent increase in GDP (World Bank, 2022). In turn, remittances have been highlighted as a powerful tool for poverty alleviation and economic development.

Africa is actively leveraging remittances as a driver for growth. The continent received over 100 billion US$ in 2022 from a global migrant workforce consisting of over 40 million individuals worldwide (RemitScope, 2023). This surpasses the formal amount of Official Development Assistance and Foreign Direct Investment flowing into the continent and has thus become a pillar for national development. In over a quarter of African countries, including Nigeria and Ghana, for example, remittance flows represent more than 4 per cent when measured against GDP (ReliefWeb, 2023; RemitSCOPE, 2023). For people on the ground, this is a valuable source of external finance to combat risks relating to food insecurity, pandemics and natural disasters while also using these funds to step out of poverty, progress through access to education and grow small businesses. Remittances have also been targeted as an outreach tool due to its ability to reach vulnerable populations. For example, it is estimated that over 50 per cent of remittances globally are sent to rural areas where the most vulnerable and food insecure populations live (IFAD, 2023).

In terms of recipients, Egypt is currently among the top five globally, and together with Nigeria and Morocco, accounted for 65 per cent of the total remittances flowing into Africa in 2022 (United Nations, n.d.).

However, sending money to, and receiving money in, Africa can be an expensive and stressful task. Sending money to support family or friends through official channels should be safe, simple and affordable. Yet, in Africa this is often not the case. According to the World Bank, sending money to Africa costs 8.5 per cent of the amount being transferred, compared to less than 6 per cent globally (United Nations, 2022). The cost of sending remittances is only one half of the battle. To receive remittances through official channels, such as remittance service providers (RSPs), people are often faced with a variety of requirements. For example, most RSPs under the RAI require remittance receivers to present proof of address, which is a crude and unreliable means of identification.[58] It is also not easily verified given that some residential areas and rural settlements have never been surveyed, and that official address systems often do not exist. Proof of address is also a poor risk mitigation tool and would become a risk if it is relied upon. Alternatively, there may be a compulsory requirement to receive remittances in person despite potentially living in an area without access to a branch.[59]

Sub-Saharan Africa is home to some of the world's most expensive remittance corridors, such as sending money to or receiving money in some East African countries (RemitScope, 2023).

KYC entails identifying and validating consumers as well as their business intents as part of a more extensive ongoing CDD effort. The purpose of KYC procedures is to proactively screen clients for risk indicators related to money laundering, terrorism financing, corruption, and fraud (Society for Worldwide Financial Telecommunications, n.d.).

CDD is a procedure that financial organizations employ to gather and assess pertinent data about a current or prospective client. It looks for anything that could put the financial institution at risk from the customer. Involves monitoring, risk analytics, and behavioural aspects of the customer and/or product in relation to the data gathered in KYC. If the customer profile changes, additional information may be required, such as proof of income or profession, in which case increased due diligence may be necessary (Society for Worldwide Financial Telecommunications, n.d.).

[58] In the remittance space, proof of address is often used as a means of identification, which is usually more effectively determined by other documents like identity proofing- or e-KYC systems and biometrics. Read more about the KYC burden posed by proof of address, in this Cenfri study.

[59] These barriers also build a case for the need to advance digital remittances, which can reduce costs and enhance last-mile access while fostering (digital) financial inclusion. Barriers to opening transaction accounts to receive remittances (typically mobile-enabled) prevent further financial inclusion.

Result: informality. Every time a remittance customer loses money or is turned away from the formal remittance system due to disproportionate KYC requirements, it drives a wedge between the formal system and the customer. Together, these challenges have forced or nudged many into using informal channels. These informal channels are deemed as more operationally efficient compared to formal channels as they do not have strenuous KYC requirements and are generally seen as more reliable by those who use them (BankservAfrica, forthcoming). Moreover, they provide better customer service, even bringing the remittance directly to the customer's home, and treat customers with dignity and respect (BankservAfrica, forthcoming). This view has permeated the African remittance market as it is estimated that 7 per cent of remittance inflows in Malawi and a staggering 81 per cent in the Democratic Republic of Congo are from informal channels (RemitSCOPE, 2023). The use of informal channels is also seen in remittance outflows, as seen in South Africa where 52 per cent of cross-border remittances to the region are estimated to be sent informally (Finmark Trust, 2021).[60] However, the use of informal mechanisms can expose a sender, provider and receiver to security, legal and corruption challenges. Thus, barriers to formal remittances limit the full potential of remittances to propel un(der)banked population in the regulated sector and form a significant development challenge for many African countries.

Many of the barriers on the receiving end are rooted in RSPs' compliance processes. By law, all RSPs are required to verify a customer's identity and assess their risk level prior to establishing a relationship (and throughout the relationship) through KYC and CDD processes, respectively. These processes are essential for combatting money laundering, terror financing and proliferation financing (ML-TF-PF). However, these processes can also create barriers to remittance access (IFAD, 2023).[61] This is especially the case for vulnerable groups such as low-income, rural households and women who are often disproportionally impacted. These barriers can arise in three ways:[62]

1. **Outdated and overly complicated regulations that do not align with international standards and best practice set by the FATF.** The FATF is the global standard-setter for measures and mechanisms to fight money laundering and terrorist financing. It provides international best practice and guidance for countries to create transparency and integrity among financial institutions and to prevent their misuse for crime and terrorism (FATF). These standards include the most up to date approaches for applying a risk-based approach (RBA), requirements for CDD and for recordkeeping. Misaligning with these best practices, or maintaining outdated practices, risks poor risk outcomes, financial exclusion and de-risking.

[60] From a study on the Mozambique to South Africa sending corridor, no respondents indicated ever having lost any money or knew people who lost money via informal channels (BankservAfrica, forthcoming).

[61] This was illustrated by the Remittance Access Initiative (RAI) recently implemented by the International Fund for Agricultural Development's (IFAD) Financing Facility for Remittances (FFR) and Cenfri (IFAD, 2023).

[62] These barriers also build a case for the need to advance digital remittances, which can reduce costs and enhance last-mile access while fostering (digital) financial inclusion. Barriers to opening transaction accounts to receive remittances (typically mobile-enabled) prevent further financial inclusion.

What is de-risking?
It is the practice where financial institutions choose to terminate or limit business relationships to avoid risk rather than managing it (FATF, 2014).

2. **RSPs' over-compliance with regulations to avoid fines from regulators.** When RSPs over-comply, by implementing requirements that are not required by law and that do not enhance the risk assessment process, it can also lead to a fixation on compliance activities that are not aligned to risk and result in financial exclusion. For example, in South Africa, some financial institutions still request proof of address for persons to open a bank account despite it no longer being required by law and despite it not being a robust identifier for verifying a person's identity (Cenfri, 2020).
3. **RSPs implementing KYC and CDD through outdated practices.** In many cases it is not the KYC and CDD that cause the barrier, but rather how these are implemented. For example, many RSPs are still verifying customer information that customers have completed on manual, hand-written forms despite already having this information on their digital back-end systems. This process risks excluding semi-illiterate customers and increasing the cost of compliance (in terms of time spent and in terms of using paper-based forms).

RSPs and regulators in Africa are well positioned to enhance remittance access, however, there is little support available to them to do so. The challenges should all be feasible to address. Yet there's limited practical guidance and capacity-building support for regulators and RSPs on how to do so. After analysing nine toolkits and guidance notes particularly targeted at RSPs and regulators, only three provided practical step-by-step guidance for enhancing remittance access. Each of these focuses on a particular entry point, such as digital financial literacy, remittance reporting systems and enhancing access to remittances for refugees. In conclusion to this research, there is no one-stop-shop toolkit for enhancing inclusive remittances in Africa. Box 4 below highlights the three available toolkits to consult for enhancing remittance access.

BOX 4: Toolkits and guides for remittance policymakers and market players

- **AFI and Cenfri (2020): Inclusive Financial Integrity: A toolkit for policymakers.** This toolkit provides an overview of what inclusive financial integrity entails and how policymakers can align financial inclusion with AML/CFT outcomes. This toolkit provides an overview of what inclusive financial integrity entails and how policymakers can align financial inclusion with AML/CFT outcomes. It also provides practical guidance on how the RBA can be implemented, how to identify financial sector risks, recommends useful AML/CFT standards and other guidance to consult and provides country examples on how to align financial inclusion with integrity objectives.
- **UNCDF (2023): A guide to assess the regional remittance policy and regulatory landscape.** This guide provides RSPs with practical guidance on which questions you should be asking when conducting a regulatory assessment and provides useful links to data sources, laws and regulations.
- **Findev Gateway (2018): Accessible and Affordable remittance services for refugees: a toolkit.** This toolkit addresses unique barriers and common issues faced by both refugees and host communities in accessing affordable remittance services. It provides practical tools for RSPs to assist with data collection and to design solutions to the barriers for refugees and FDPs.

5.2 Deep dive 2: Developing and implementing your own innovative intervention to address KYC and CDD barriers

Start by considering the remittance context. The first step is to conduct some brief desktop research to understand recent developments and changes in the economic and policy context that impact the remittance market. Key to this process is identifying the size of the potential target market, how the financial institutions in the country are perceived in the international market, and whether any upcoming changes to regulation could impact innovation. The box below provides an example of how you can understand your country's context, using an example from The Gambia.[63] For an individual RSP, this involves looking at the following:

- **Updated data on the number of remittance senders and receivers** and customer segmentation to assess your market share and identify the size of the opportunity to expand.
- **The national strategy for financial inclusion and policy objectives related to leveraging remittances for development.** If remittances are a national policy objective, then there is likely more support for innovation.

[63] The Gambia was chosen due to its inclusion as an IFAD PRIME country.

- **The SDGs**,[64] to better understand how your innovation can contribute to reaching them. Remittances and innovative approaches toward increasing access to remittances can contribute to meeting 10 of the SDGs. See IFAD's Remittances, investments and the Sustainable Development Goals for more information.
- **Updates on any financial sector policy changes or initiatives** that are intended to realign the financial sector or support other national policy objectives. These could provide potential avenues of innovation that support change in line with current SDGs.
- **FATF country status**, to understand the state of the country's AML/CFT framework or evidence that your country is at increased risk of entering global watch lists (click here to find your country status). Recent updates and guidance by the FATF would also be useful to consult. This will indicate how financial institutions in your country are being perceived by international partners and correspondent financial institutions, particularly concerning weaknesses identified in mutual evaluations.

BOX 5: Example of understanding the country context using The Gambia's remittance data

- The Gambia relies quite heavily on remittances. Up to 47 per cent of households indicate a dependency on remittances in The Gambia (International Monetary Fund, 2021).
- 33.2 per cent of individuals in The Gambia are financially excluded. This represents a 50 per cent reduction in financial exclusion from 2019 and is likely influenced by the emergence of mobile money services and the entry of new digital players.
- Since the financial exclusion rates are still relatively high, this had led to a practice of receiving remittances in cash at physical locations, as opposed to digitally through bank accounts or mobile wallets (RemitSCOPE, 2023).
- There is therefore ample scope to enhance financial inclusion and increase the use of digital methods for receiving remittances.

Next, assess the regulatory environment. The regulatory framework sets the boundaries within which market players operate. The next step in identifying potential innovations to implement is to understand the regulatory environment in which an RSP operates, and how that shapes the scope for innovation. This is done through desktop research and discussions with key role players, such as regulatory liaisons, industry bodies and associations, civil society groups with interest in remittances and other global organizations, e.g. IFAD. The purpose is to identify the parameters, the opportunities for innovation, and the risks and any contradictions associated with the regulatory framework. This step is essential for all financial institutions to identify areas for opportunity to innovate.

Regulators can also benefit from conducting a regulatory analysis, as it can help them to identify opportunities to align with international best practice

[64] To read more about how remittances can support the SDGs, click here.

and, where relevant, shape their strategy to avoid typical risks and pitfalls in compliance.

Chapter 2 provides a step-by-step guide on how to conduct and apply a regulatory analysis for RSPs, while **Deep dive 3: A guide for regulators to assess regulations against inclusive integrity goals and best-practice** provides guidance for regulators.

Finally, place your RSP in this landscape by considering to what extent you have the autonomy to implement innovative interventions. Implementing a remittance access innovation requires time, resources and commitment. Not all RSPs are in a position – or have the motivation – to do so.

It's time to identify the relevant barrier(s). Barriers to remittance access are often a manifestation of incorrect or improperly implemented KYC and CDD by RSPs. These barriers have a myriad of negative consequences, including but not limited to excluding people from accessing their remittances, increasing the cost of compliance, and even negatively impacting the customer experience. Barriers to remittances can present in various ways. To identify these, RSPs can look at whether their customers can easily access their remittances, the documentation requirements they impose on them, and how they risk rate their customers.[65] Key questions to ask yourself as an RSP representative include:

- Is my organization requesting any form of ID for a remittance transaction that is not required by law? (for example, proof of address)
- Are customers not coming to collect their remittances? If so, why not? Are they illiterate? Do they live too far away? Is there a language barrier?
- Are customers complaining about having to share too much personal information (specifically information that's not required by law)?
- Are customers complaining of long waiting times and inconvenient processes?
- Are customers unable to access their remittances because they forgot, lost, or damaged their ID, despite being a loyal customer/having used your remittance services before?

Answering yes to these indicates that you are experiencing barriers to remittances within your organization. An example of a barrier would be requesting proof of address as a form of verifying a customer's identity, where it is not required by law. Proof of address is not a reliable identifier, is costly and time-consuming for RSPs to verify, and few customers have proof of address.

[65] For further reading on market-related barriers to remittances, you can read the Cenfri report here, or the IFAD remittance market diagnostic reports here.

The next step is to devise an innovation to align with the key barrier(s). Based on the barrier you identify; you can then develop an innovative intervention to address this. To draw on the example of proof of address as a barrier above: an innovative intervention would be to remove this requirement and strengthen the KYC process by introducing more reliable measures such as biometrics to verify identity. It will be essential for you to think through the implications. Each intervention discussed in chapter 3 is complemented with an overview of the resources you'll need to implement it and a guide on how to measure the intervention's impact. The information provided there will support you in developing your own innovative intervention implementation plan in which you will need to answer the following:

- **How does this intervention align with your strategic objectives?** Will the intervention be implemented on in-house remittance products, or partner products as well? Is the intervention aligned with your core key performance indicators (KPIs)?
- **Which resources will you allocate to this project?** How many resources (how many people, how much of their time, and in what capacity) will likely be required? Is this feasible to implement given other budget priorities? What is the timeline associated with this intervention? Are any specific skills, like software development, needed for this intervention? What other intervention is going on or is planned that impacts this intervention? How can these be aligned or sequenced to optimize resources and capacity?
- **How will you resource this project?** Do you wish to outsource the implementation of the intervention or do it in-house? If you outsource, which components do you outsource to balance with internal ownership? If doing it internally, do you need some internal training and on what aspects?
- **What is the timeline commitment and what is the scope of this project?** Do you think that you will be able to complete this intervention along with your other priorities? Does the selected intervention accurately address your customers' challenges regarding remittance access? Will the intervention be implemented only on in-house remittance products, or partner products as well?
- **Who is impacted by this project and how should you consider them?** Will customers be interested in this intervention? Do you need to consider ways to generate interest around the intervention among your customers? How interested are the IMTO partners in implementing it within their processes?
- **What is your desired impact with this project?** How does the intervention benefit vulnerable customers, improve regulatory compliance and impact the bottom line? What KPIs for success will you set?

Now it's time to generate support from relevant stakeholders. Two key groups will be essential for any changes you intend to make:

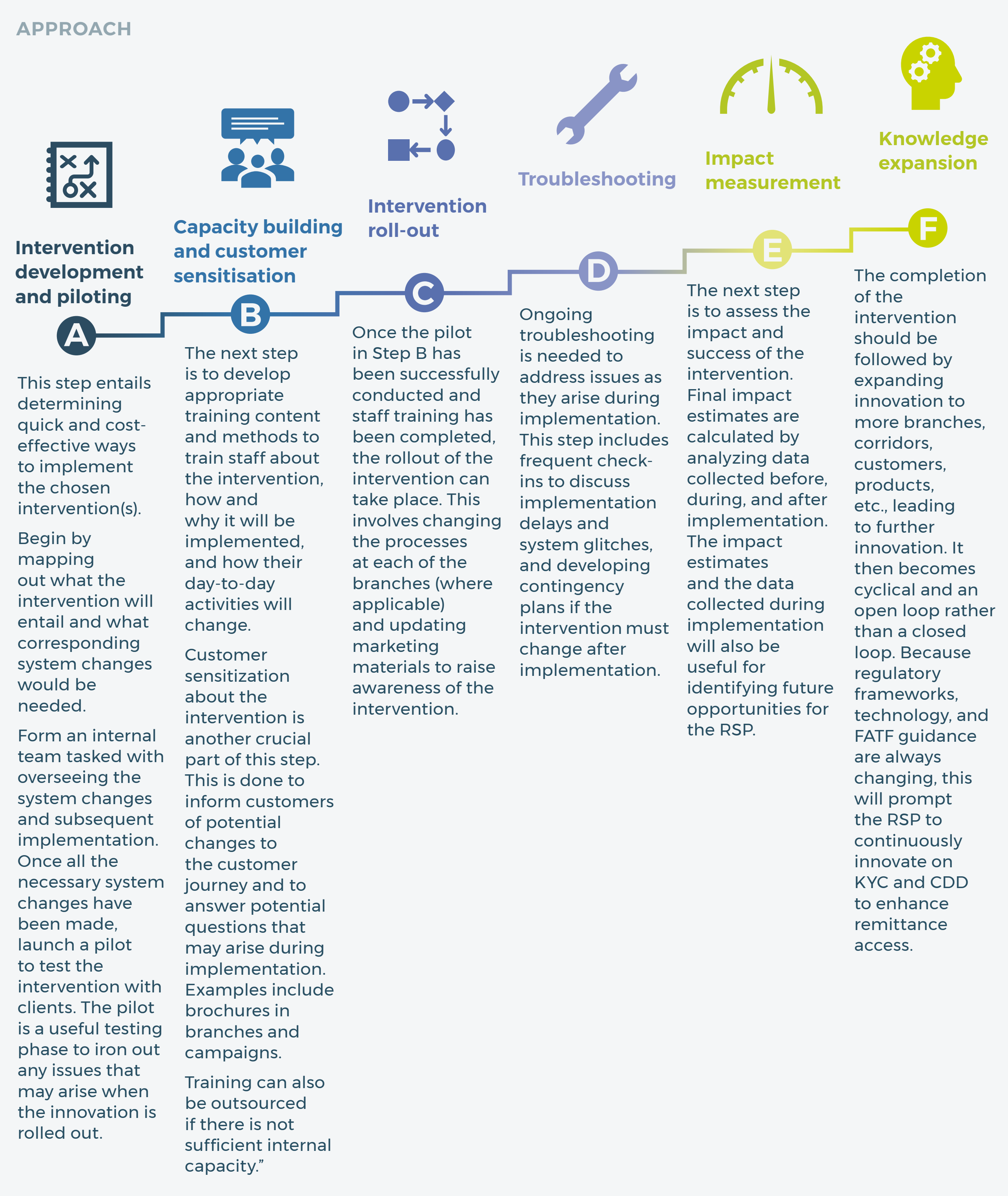
- **Obtain the necessary buy-in and support from RSP management.** Once you've got a solid grounding of your remittance landscape, and you've identified a challenge that's within your scope to address (alongside an innovative intervention to address it), you'll need to pitch the innovation idea to key internal stakeholders. This is an essential step for generating internal awareness, buy-in and creating alignment in expectations. Start by reaching out to relevant parties and/or departments to notify them of the intent to innovate to improve remittance access and agree to collaborate on the process. Also, secure the involvement of top management. In some cases, you may need to have the intervention plan signed off by the heads of relevant departments, whereas in other cases a verbal confirmation will suffice; this depends on the particular RSP's structure.

Key teams to get buy-in from:

- Compliance and risk
- Product development
- Business development

- **Consider involving the regulator early and bring them up to speed.** The close interplay between remittance access innovations and the regulatory framework means that it is important that the regulator is informed of the planned innovation, and of its progress as it proceeds. You can inform the regulator by sharing a notice with them or setting up quarterly engagements to allow them to suggest improvements to interventions. Regulators' openness to engage varies depending on the progress or lack thereof on a risk-based approach and risk-based supervision as well as available mechanisms for engagement between RSPs and regulators, among other factors. Chapter 2 of this toolkit provides strategies for RSPs to actively communicate with the regulator.
- **Based on the above, you can now map out the innovation intervention journey.** The final step is to start to plan for the intervention by mapping out the different steps in the implementation process. It is important to be realistic about the expected timeframe. In the RAI programme, the implementation journey per RSP spanned between six and eighteen months. The figure below provides an indicative overview of an intervention implementation journey.

FIGURE 7: STEPS IN THE INNOVATION JOURNEY



APPROACH

Intervention development and piloting

This step entails determining quick and cost-effective ways to implement the chosen intervention(s).

Begin by mapping out what the intervention will entail and what corresponding system changes would be needed.

Form an internal team tasked with overseeing the system changes and subsequent implementation. Once all the necessary system changes have been made, launch a pilot to test the intervention with clients. The pilot is a useful testing phase to iron out any issues that may arise when the innovation is rolled out.

Capacity building and customer sensitisation

The next step is to develop appropriate training content and methods to train staff about the intervention, how and why it will be implemented, and how their day-to-day activities will change.

Customer sensitization about the intervention is another crucial part of this step. This is done to inform customers of potential changes to the customer journey and to answer potential questions that may arise during implementation. Examples include brochures in branches and campaigns.

Training can also be outsourced if there is not sufficient internal capacity.”

Intervention roll-out

Once the pilot in Step B has been successfully conducted and staff training has been completed, the rollout of the intervention can take place. This involves changing the processes at each of the branches (where applicable) and updating marketing materials to raise awareness of the intervention.

Troubleshooting

Ongoing troubleshooting is needed to address issues as they arise during implementation. This step includes frequent check-ins to discuss implementation delays and system glitches, and developing contingency plans if the intervention must change after implementation.

Impact measurement

The next step is to assess the impact and success of the intervention. Final impact estimates are calculated by analyzing data collected before, during, and after implementation. The impact estimates and the data collected during implementation will also be useful for identifying future opportunities for the RSP.

Knowledge expansion

The completion of the intervention should be followed by expanding innovation to more branches, corridors, customers, products, etc., leading to further innovation. It then becomes cyclical and an open loop rather than a closed loop. Because regulatory frameworks, technology, and FATF guidance are always changing, this will prompt the RSP to continuously innovate on KYC and CDD to enhance remittance access.

5.3 Deep dive 3: A guide for regulators to assess regulations against inclusive integrity goals and best practice

This deep dive provides a guide for regulators in their quest to align regulatory frameworks with inclusive integrity principles and international best practices as set by the FATF and other standard-setting bodies. In doing so it covers the following steps as sub-sections:

1. Defining inclusive integrity goals;
2. Aligning with international best practices;
3. Amending the regulatory framework accordingly; and
4. Measuring the success of inclusive integrity.

DEFINING INCLUSIVE INTEGRITY GOALS

The point of departure for any regulator wanting to do a stock-take of their own regulatory framework is to define the goals for inclusive integrity in the local context. This consists of three steps:

Step 1: Understand and explicitly recognize the interplay between financial inclusion and financial integrity.[66] Key standard-setting bodies such as the FATF and the Alliance for Financial Inclusion (AFI) have acknowledged that complying with global AML/CFT standards should not come at the expense of financial inclusion. In fact, they promote implementing effective AML/CFT regimes that take account of financial inclusion objectives, thus advancing these two agendas together (AFI, 2020). Based on this, they have set several standards and provided guidance for regulators and policymakers to merge and jointly pursue these two agendas. Thus, to align with international best practices, regulators must recognize, understand and commit to pursuing *inclusive integrity* as the ultimate objective. AFI (2020) describes the ultimate success of inclusive financial integrity as:

> "…a situation whereby **a safe financial system that** has adequate and effective measures in place to identify, assess, understand and mitigate ML-TF risks and to act as soon as the risks have been detected, **is equally able to provide greater access to and usage of quality formal financial services** in a way that enhances livelihoods and drives sustainable development."

Step 2: Define national goals for inclusive integrity. Once you understand the inclusive integrity concept, it is important to contextualize and embed it in your national goals and objectives. Defining objectives for inclusive integrity is a deliberate process that requires a good understanding of the financial inclusion goals and objectives in the local jurisdiction, for example as contained in the National Financial Inclusion Strategy or other similar policy documents. While

[66] Addressing financial exclusion and strengthening the financial system have long been viewed as two distinct objectives. In fact, many have pursued one at the cost of the other. For example, to strengthen the robustness of the financial system, many countries have imposed stricter requirements on their financial institutions, which have led to stricter requirements on customers. This has often resulted in low-income; low-risk and vulnerable communities being excluded simply because they don't have what they need to comply.

defining these objectives, also (1) determine which broader policy objectives and key performance measures align with the objectives for inclusive integrity; and (2) which will detract from these objectives. This will enable you to make trade-offs between less important objectives and those that will be key focus areas, and to interpret the risk of exclusion as both an inclusion and an integrity goal. An example of such a national inclusive integrity objective is to reduce access- or usage-related barriers to remittances for low-income and rural households.

TIP Implement a national regulatory impact assessment to identify areas for development and inform inclusive integrity goals. Defining your national inclusive integrity goals can be challenging. If you do not already have goals in mind, or if you're not clear on how achieving these goals could impact other components in the financial sector, then it may be best to conduct a regulatory impact assessment. This process will allow you to assess the strength of your existing regulations, identify strengths and weaknesses and shed light on gaps and opportunities for inclusive integrity. Based on this assessment, you will then be able to synthesize key insights from which to develop your inclusive integrity goals. The box below provides more information on how you can conduct such a regulatory impact assessment.

BOX 6: Conducting a regulatory impact assessment to accompany goal setting and determine what success looks like

A common mistake that many regulators make is neglecting to review previous legal documents within the regulatory framework, specifically to learn from what did not work and identify key gaps that a new legal document can address. Such a review should start with the regulations in the country and then also include examples of regulations in the region.

A regulatory impact assessment allows you to critically assess all effects (both positive and negative) associated with existing regulations. This assessment ties in with following an evidence-based approach to policymaking, which assists regulators in basing decisions on whether to adapt or write new laws and regulations based on facts and evidence (OECD, 2020).

There are various methods for conducting a regulatory impact assessment. The right method for you will be determined based on your specific goals. Some examples of methodologies as outlined by the OECD include:

- A least cost analysis which looks only at the costs of the regulation.
- A cost-effective analysis which entails regulators quantifying the benefits generated and dividing it by the cost to society.
- A cost-benefit analysis, which entails the monetization of all costs and benefits compared to the most viable alternatives.
- A multi-criteria analysis, which allows a comparison of alternative policy options against pre-determined criteria, e.g. the impact on low-income and rural households, or whether there are other regulatory instruments you could have used to achieve the same impact.

In addition to assessing the impact of existing regulations, it is also advised to apply this approach before you draft new regulations to determine the potential advantages and disadvantages of the proposed regulations. Ongoing measurement of the effectiveness of regulation can reduce the cost and time implications of the regulatory impact assessment for new or amended regulation.

Note that a regulatory impact assessment is often done on the regulation's initial goals, but it is important to do it on the changed or evolved objectives for inclusive integrity. The benefit of such an assessment is that you can keep the original regulation's foundation while making various amendments to adjust the regulation to the new objectives.

The use of data to support a regulatory impact assessment: When conducting the assessments above, it is essential to use data to determine the impact of your policies, particularly the impact on vulnerable groups. This will enable you to measure the success of meeting your objective, like financial inclusion. Since vulnerable groups often fall victim to fraud and abuse, having access to such data can enable you to identify loopholes where your system is potentially being abused. For instance, an alert that a known rural person's ID is unusually being used to send remittances in an urban area or vice versa. If you wish to incorporate such data into your impact assessment, you can start by using the national lists published by your National Bureau of Statistics which segments urban and rural areas to determine which people fall within each classification.

Step 3: Determine what success looks like in your context. The final step in defining inclusive integrity goals is to determine what will constitute success in meeting these goals, or what the measurable indicators of success will be. This approach is not only effective for measuring whether you have met your goals but is also in line with the principles-based approach as mandated by the FATF, as the principles-based approach focuses on *outcomes*. Defining what success looks like provides direction on what is most important and ensures that resources are allocated accordingly. Continuing with the example objective that you have set in Step 2 above, success in this case would be ensuring unhindered remittance access for customers including low-income and rural customers. Setting this as the measurable outcome requires defining requirements in terms of what needs to be achieved (for example, the number of customers for which identity is effectively verified) rather than focusing on the inputs, or what information is required from customers. For example, when it comes to which identifiers are required from customers, the regulatory framework should require institutions to identify and verify identity using independent information or documents as per the FATF's guidance. However, the regulation should not specify the need to collect specific documents, e.g. only government-issued documents.

ALIGNING WITH INTERNATIONAL BEST PRACTICE

International standards and guidance provide ample direction for following a risk- and outcomes-based approach that allows inclusive integrity goals to be met. The next step in the journey for regulators wanting to do a stock-take of their own regulatory framework considering inclusive integrity goals is therefore to see how best to align with international best-practice. To do so, there are four relevant steps:

Step 1: Identify international best practice relevant to your goals. Once you have set your inclusive integrity goals and you know the outcomes that you want to work towards, you will need to identify mechanisms to leverage to help you get there. International best practice, standards and guidelines, as developed and published by key thought leaders, policy-setting bodies, regulators and other international organizations, offer the most appropriate and most advanced mechanisms for achieving inclusive integrity goals. A simultaneous advantage of leveraging these is that it enables you to spend less time on playing "catch up" to other countries by informing you of the latest innovations and requirements. Figure 8 below provides a non-exhaustive list of some of these documents that are available to be consulted:

FIGURE 8: **BEST PRACTICE RESOURCES TO CONSULT**

1. Publications by the **FATF** including the 11 immediate outcomes, the key FATF **recommendations** and FATF guidance, e.g. the guidance on digital identity (2020)
2. **European Union** directives, e.g. those on anti-money laundering and terrorist financing
3. Guidelines by the **Bank of International Settlements**, such as these risk management guidelines
4. Guidelines and other regulatory documents published by other **countries** who have tackled issues similar to yours, e.g. South Africa's Guidance Note 7
5. **Other toolkits** that can serve as practical guides for how to address specific challenges you may face, e.g. Cenfri & AFI's toolkit on inclusive financial integrity

Step 2: Draw out the key learnings as per your objectives. Based on the inclusive financial integrity goals that you set, you will need to engage with best practices in a way that is fit-for-purpose and meets your specific needs. For instance, if your objective is to encourage innovation around the use of digital identity, then your next actionable objective is likely to update your existing regulations or draft new ones. With this objective in mind, you will look at publications specifically about identity, e.g. the FATF's guidance on digital identity, and draw out key recommendations and learnings for you to incorporate when adjusting your own regulation. These best practices serve as a starting point, or practical example, for any country.

Step 3: Acknowledge your context. As you are drawing out key elements from the best practices which you can implement, it is important to acknowledge the local contextual realities, as, depending on where the country is at, aligning with international best-practice may mean that some basic building blocks first need to be put in place. For example, the FATF's guidance and best practice starts with recommending that all countries transition to the risk- or principle-based approach to AML/CFT (see section 2.2 for more information on the rules- vs. outcomes-based approach). All subsequent recommendations and guidance are premised on the notion that the country consulting the material has already started the transition and is now furthering their journey. Therefore, how you internalize your learnings will depend on where you are in this journey. If you are currently following a purely rules-based approach, the changes that you implement to move towards a risk-based approach will differ from a regulator who is already following more of a risk-based approach. The section “Amending the regulatory framework” below provides an outline of how to align your regulation with the outcomes-based approach.

Step 4: Identify key aspects of regulation that could benefit from a move to a principles- and risk-based approach. A final step in the process to align with international best-practice, is to determine key sections in your regulation to which you can apply a more principles-based approach. This can, for example, include how you outline risk management policies, recordkeeping requirements, due diligence requirements, or which identification documents you require (these are further discussed in table 29 in the next sub-section). Doing so will enable you to get a clearer view of the changes required, either by amending existing regulations or drafting new ones.

The next sub-section provides a practical guide to amend your regulatory framework in line with the learnings from your research on international best practices.

AMENDING THE REGULATORY FRAMEWORK

Once you have defined your inclusive integrity goals and taken stock of what needs to happen to align with international best-practice considering the local context, the next step is to amend the regulatory framework accordingly. There are four steps to follow in this regard:

Step 1: Understand the key types of risks to be on the lookout for. A key starting point for amending the regulatory framework to better align with international best practices, is to understand the key risks that can manifest in any financial sector. Different types of risks, such as money laundering risk and terror financing risk, are often confused and/or conflated, not only by RSPs but also by regulators. Thus, the first step is to make sure that you have a clear idea of the different types of risks and how they can manifest. Table 27 below provides a summary of some of the key and common risks to be on the lookout for:

TABLE 27: **KEY RISKS RELATED TO FINANCIAL INTEGRITY**

National risks related to financial integrity	
Compliance risk	Refers to noncompliance with legal regulations, industry standards, guidelines, internal policies and regulatory obligations poses a risk, potentially leading to fines, penalties and damage to the reputation of financial service providers (FSPs) (Alliance for financial inclusion, 2020).
Illicit financial flows risk	Illicit financial flows (IFFs) are the illegal transfer or smuggling of people, wildlife, resources and money across international borders and within trade systems. IFFs can significantly affect development outcomes by depleting national resources, displacing capital, ingraining a short term rents seeking business culture and lowering government tax income (Alliance for financial inclusion, 2020)

National risks related to financial integrity	
Money laundering risk[67]	The possibility that a nation, financial institution, or corporate division will be exploited for money laundering (Alliance for financial inclusion, 2020).
Proliferation financing risk	Involves the potential of obtaining, transferring, or providing funds, assets, or economic resources, either entirely or partially, to individuals or entities for specific purposes (FATF, 2021).
Risk of financial exclusion	Is described as the risk of rejecting consumers because there is insufficient AML/CFT data runs the danger of depriving individuals of financial services, which can spark the emergence of sizable unregulated informal sectors. This is a weakness where money laundering and other criminal activities could be facilitated (Alliance for financial inclusion, 2020).
Terrorist financing risk	The possibility that a nation, financial institution, or company could be used for terrorist financing (Alliance for financial inclusion, 2020).
Trade-based money laundering risk	Trade-based money laundering risk refers to the potential for criminal organizations and terrorist financiers to exploit the international trade system as a means of disguising the proceeds of crime and integrating illicit funds into the legitimate economy. This risk arises from various factors within the trade system, including the vast volume of trade flows, complexities associated with foreign exchange transactions and trade financing arrangements, the commingling of legitimate and illicit funds, and limited resources available to customs agencies for detecting suspicious trade transactions (FATF, 2006)

Step 2: Identify the risks specific to your jurisdiction. Once you have a clear understanding of the types of risks, the next step is to identify and prioritize those risks that are most prominent in your jurisdiction. These risks are the key gaps that can be addressed by better aligning with international best practice. The stakes are high – **if not effectively mitigated or addressed, such risks can result in a country being placed on enhanced/increased monitoring by the FATF**. This is more commonly known as being placed on the grey list. *Grey listing* entails being placed on the FATF's list for increased monitoring due to perceived inadequacies in combating financial crimes, indicating a shortfall in meeting international standards. Once grey listed, a government commits to an action plan to address deficiencies identified in the AML/CFT mutual evaluation. The FATF monitors the plan's implementation within a specified timeframe, and then determines whether to allow the country to graduate from the list. While this may seem fairly simple, the process to graduate from the list can be resource intensive, and the consequences of being on the list have been known to include significant reputational damage and even de-risking (National Treasury, 2023).

This report recommends two ways of taking stock of specific risks in your jurisdiction: the first is through conducting a national risk assessment and the second is to consult the most recent mutual evaluation report (MER) conducted by the FATF and follow steps to address the deficiencies noted. Both are discussed below.

[67] In addition, the risk of fraud entails the risk of corrupt agreements that include extortion from or collusion with other individuals, or it can encompass the falsification of financial or other records within a company (Deloitte, n.d). Although not a direct financial integrity risk, the risk of fraud is a predicate offence for money laundering. The goal should be to spot fraudulent activity so that you can understand the money laundering implications.

1. CONDUCTING A NATIONAL RISK ASSESSMENT

There are three options for enhancing or conducting a national risk assessment (NRA) to ensure that you are identifying and prioritising the risks most prominent in your jurisdiction, and that you are introducing effective risk mitigation strategies:

i. The first option is to **upgrade and refine your existing national risk assessment.** This entails ensuring that your risk assessment accounts for, and assesses, the potential impact of new and relevant risks emerging and manifesting within your jurisdiction, region and in the global market. This includes but is not limited to changes in the weights and levels of inherent risks and variation in their modalities. It also involves taking stock of illicit flows, trade-based money laundering, illicit wildlife and resource trafficking and human trafficking in your jurisdiction and region and the resultant impact on the levels and current mix of risks encountered. Once you've revised your list of risk types and -factors, it is essential to consider how these new risks may interact with and impact inherent MF/TF/PF risks within your country context. For example, the risks flagged here are of particular importance for resource rich countries (such as oil, gas, human resources, diamonds, etc.) where risks associated with resource trafficking may be exacerbated by ML or may advance TF.

ii. If your country is not already applying an internationally robust NRA model, then the next option is to **consult and leverage reputable models** of comprehensive risk assessment frameworks as basis for developing an NRA. No single model will be a perfect fit, so it becomes important to review the different models as they emphasize different aspects that may be better suited to your own context. It is critically important that any model applied needs to reflect the nuance and specific requirements of your jurisdiction. Never force-fit the complexity of your jurisdiction to reflect well in a global model. Various models can be used as basis for a national risk assessment. For example, both the International Monetary Fund (IMF) and the World Bank have national risk assessment models for regulators to consult. While both are robust and well informed, the World Bank model is better suited for developing countries' risk realities. These models are not available in the public domain but can be accessed in consultation with these institutions. Key to note here is that such models should not be applied in a tick-box fashion or as a template. If you decide to consult these models the point of departure is to collect, import and analyse data so that you can assess what (a) the types of risks are in the local context; (b) the incidence of each; and (c) what mitigation is in place, and to do that assessment in the local context. Thus, these models should be implemented based on an empirical evidence base to ensure that it is tailored to the national context. The burden needs to be placed on institutions to each understand and document their own risk, which then gets added up into a national risk assessment.

iii. The third and final option is to **conduct a sectoral risk assessment.** This approach allows each sector to conduct their own sector-wide risk assessment and then report their primary and most prominent risks to the regulator to be coordinated and collated. For example, Ireland's 2019 NRA was conducted as a sectoral approach. It included a review of

22 sectors based on quantitative and qualitative inputs. It consulted various models, including the models and methodologies of EU and non-EU countries, the FATF guidance, the World Bank and IMF models. A key element was the extensive consultation with public and private sector stakeholders. This provided Ireland with a tailored approach that was fit-for purpose for their own context (Anti-Money Laundering Section, 2019). While this approach has had success in wealthier countries, and it can relieve some capacity pressure on the regulator, it can also introduce new hidden risks related to limited oversight, inconsistent and incorrect understandings of risk, and varying degrees of quality (based on the capacity and skill housed in each sector). For this approach to have value, sectoral inputs need to change from a consensus basis to an empirical basis, like the Ireland NRA quoted above (i.e. rely on quantitative and qualitative data and information, not on perceptions). This is easier said than done, because it requires capacity to collect, track and analyse data consistently across all sectors at a granular level.

2. ASSESSING YOUR MUTUAL EVALUATION REPORT

A country's MER provides an assessment of that country's strategic deficiencies and areas that require improvement. It may even provide recommendations on how to address these. Depending on the severity of these risks, the FATF may warn or place a country on the grey list. During this step, you should comb through the mutual evaluation reports and progress reports (if applicable) and review the key deficiencies and immediate outcomes outlined, within the correct context. Questions to ask are: (a) what has changed in the FATF context or focus; and (b) how we can address these key deficiencies in a forward-looking way. Box 7 below provides a case study on the process to follow if your country is on the FATF's grey list.

BOX 7: Your country is on the FATF grey list. Now what?

Enhanced monitoring, or being placed on the grey list, is a consequence of not effectively addressing risk in your financial sector. If your country is on the FATF grey list, this means that the FATF has found that it had strategic deficiencies, and that the country has undertaken a high-level political commitment and plan to address this. Practically, such countries are likely subject to much greater scrutiny and may start feeling the economic consequences if countries and the global financial sector are no longer confident to conduct business with them, for fear of impacting their own global standing (a phenomenon known as de-risking). The rest of this box provides a step-by-step guide on measures to help a country get off the grey list.

Step 1: Understand your mutual evaluation report. The first step to moving off the grey list, is understanding why you were placed there in the first place. This involves reviewing the deficiencies and recommendations in the MER with scrutiny to determine exactly where the gaps lie that you need to address. At the start of each chapter, a summary section called "key findings and recommended actions" outlines the most important findings. Thereafter, you can review specific sections, e.g. national AML/CFT policies and coordination in more depth. Next, you will navigate to the Technical Compliance Annex where you can find recommendations which should be built into regulation. You can again first read the summary of the key deficiencies and then review specific recommendations in depth. These include recommendations on customer due diligence, record keeping and applying the RBA, among various others. Follow-up reports are frequently published by regional FATF-style bodies, and those recommendations and key findings should also be reviewed.

Step 2: Revisit the national risk assessment. Countries should not include risks in their national risk assessment without ensuring that each risk has a sound empirical foundation for being quantified and included. Consulting data to inform risk ratings is a good starting point to prevent this. If there are unnecessary risks included in the national risk assessment, or if there are risk ratings that are informed by perception only, this can signal to the FATF-Style Regional Bodies (FSRBs) that the country does not accurately understand the risks they face and therefore likely does not effectively mitigate risks.

Step 3: Revisit empirical evidence coming from the financial sector. Encouraging industry players, e.g. RSPs, to collect and report data is a crucial part of more accurately understanding the industry and the risks you face. Use this data to better understand the market and to better manage risks.

Step 4: Depoliticize regulatory reform. Regulators and public authorities should steer away from bringing political agendas into the regulatory reform. This can unnecessarily drag out the timeline of changes in the regulation, thereby resulting in a longer time spent on the grey list. Instead, support should be provided from all parties involved to make the necessary changes quickly and efficiently. The quicker countries can move off the grey list, the less the risk of reputational and economic consequences and of moving to the blacklist will be.

TIP Steer clear of "quick fix" solutions, like using international regulatory templates. These lack country context and are guaranteed to do more harm than good. A concerted effort from all regulatory parties and related stakeholders will have a more desired outcome.

Country case study on Ghana's removal from the grey list[68]

- Ghana was first placed on the FATF's grey list in 2012 due to their high risk for ML and TF (FATF, 2012). Although they made progress on addressing their AML/CFT deficiencies, by 2016, significant gaps remained which led to Ghana being placed under observation by the International Cooperation Review Group (Ghana Ministry of Finance, 2021).
- To address these deficiencies, Ghana and the FATFs The FATF's International Co-operation Review Group (ICRG) developed a two-year action plan from 2019–2021. During this time, despite economic turmoil fuelled by both internal and external factors, Ghana remained committed to graduating from the grey list and developed several national policies to address the deficiencies outlined by the FATF. A few of the changes made to address these deficiencies include, among others, based on the findings from previous mutual evaluations, a) establishing a specialized unit within the National Intelligence Bureau to investigate all TF related cases, especially those in relation to the non-profit organization sector; and b) published an updated AML Act in 2020, which addressed deficiencies related to provisions for financial sanctions (FATF-GAFI, 2022).
- In 2021, Ghana was removed from the grey list as they had met with FATF's requirements to address key deficiencies in their AML/CFT framework. Their successful removal from the grey list highlights the value of a country-wide collaborative effort, which included the Ghana Revenue Authority, Bank of Ghana, the National Intelligence Bureau, the Ghana Financial Intelligence Centre and more, to address the various AML/CFT deficiencies. The process undertaken in Ghana has not merely remedied deficiencies, it has become a positive case study, changing the trajectory of the Ghanaian financial sector both within the region and internationally.

[68] Ghana was chosen as country example due to its inclusion in the IFAD PRIME countries.

Enhance step 2 by assessing your own approach to risk and overcoming fallacies associated with the no-tolerance approach. As discussed, promoting a *no-tolerance* approach to ML/CF/PF is thus not technically possible. In fact, stating that you have zero risk tolerance may send signals to the international market that this jurisdiction may be applying a blanket approach to all risk, thus in fact, making it a higher-risk country. The correct approach is to see mitigation measures as tools to effectively identify and manage specific local risks in alignment with that country's risk appetite. This is a core component of the principles-based approach; acknowledging the presence of risk and formulating the regulatory authority's risk appetite is already a step in the right direction to ensure that legitimate consumers and the local economy are supported.

Step 3: Updating your local regulatory framework to address the key deficiencies. In step 2, you took stock of the key deficiencies and gaps from a risk perspective, which has provided you with insight on what needs to be changed. This step is focused on developing an appropriate approach for mitigating the risks identified and/or addressing the key gaps in alignment with your national objectives and inclusive integrity goals, through updating the local regulatory framework accordingly. Start by thinking about which areas of regulation to update and by consulting the market. This will ensure that regulation is highly practical and implementable.

Ideally, changes to regulations should be industry-led and regulator-approved.

Table 28 below provides an example of how to move from a rules-based approach to KYC and CDD to a principles-based approach. The example assumes that the hypothetical country has outdated regulations that require amending, or that need to be rewritten, which creates an ideal time to incorporate innovative approaches to enhance inclusive integrity:

TABLE 28: MOVING FROM A RULES-BASED APPROACH TO A PRINCIPLES-BASED APPROACH

If you are here:	You should do this:	To get to this:
Rules-based approach Country Y's **due diligence obligations** are framed in a **rules format**. In this case, the due diligence approach to be followed depends on **whether the customer can provide all the required information**, e.g. proof of address, occupation, the purpose of transaction, etc.	Incorporate elements from the **risk-based approach** as mandated by the FATF. Instead, Country Y should focus on requiring that financial institutions undertake proportionate due diligence. This means applying documentation **requirements that align with the real risks** (informed by data) posed by the customer.	**Principles-based** approach This can allow for a more **principles-based approach** to consider which attributes are relevant as they inform risk. In the end, this **moves away from setting a rule** to be followed, **to establishing a principle** that a financial institution should implement as they see fit **within their context**.

Step 4: Leverage this approach to usher wider innovation into the market. Some of the areas for improvement in your regulatory framework can help to enable RSPs to innovate within the market – as is outlined in chapter 3. Some of the suggestions for regulatory amendments to enable innovation are listed below in table 29:

TABLE 29: POTENTIAL REGULATORY AMENDMENTS TO ENABLE INNOVATION

Requirement	Recommended regulatory amendment in line with a principles-based approach[69]	Law or regulation affected	Corresponding intervention in Chapter 3
Make record-keeping more flexible	RSPs to keep records on identification data collected throughout the CDD process (e.g. copies or records of official identification documents like passports, identity cards, etc.) for 5 years (in line with FATF requirements).	AML/CFT acts, laws, regulations & directives, guidelines	Customer profile Replacing manual forms with printed receipts
Be flexible on required identifiers	Remove the prescription of identifiers for KYC and CDD in line with the outcomes-based approach. Instead, add that identity should be verified in a risk-controlled or -appropriate manner.	AML/CFT Acts, regulations and guidelines	Risk assessment
Not requiring new KYC and CDD for every (repeated) transaction	Rely on the identification and verification steps undertaken for past encounters with the same customer unless there are doubts on the accuracy of the information.	AML/CFT act, regulations, guidelines	Digital ID database
Enabling remote onboarding	Specify that digital ID systems can be used to enable remote ID verification and support remote financial transactions at standard or lower levels of risk.[70]	AML/CFT law and relevant circulars	Agent expansion and management models

MEASURING THE SUCCESS OF INCLUSIVE INTEGRITY

The final element in aligning the national regulatory framework and approach to local goals and international best practices is to have a framework in place for monitoring progress towards the developed inclusive integrity goals. This has five steps:

Step 1: Establish a monitoring and evaluation framework based on your objectives. A first step towards measuring the success of your regulation in meeting its inclusive integrity goals, is to set up a monitoring and evaluation (M&E) framework which can track the progress of how these objectives are being met. An ideal M&E framework includes the overall goal of the regulation, the planned outcome, as well as the associated outputs with the regulatory change. For example, if you are amending a regulation related to the identifiers that are allowed for a remittance transaction:

[69] For all 40 updated recommendations published by the FATF, click here.

[70] Specific assurance measures should be built into the regulation. Reference can be made to the FATF guidance on digital identity measures, and specifically Appendix E (FATF, 2020).

- **The goal** may be to (a) move towards a more principles-based approach and (b) allow for the use of more alternate identifiers,
- **The output** will be the amended regulation and may include further guidance to support practical implementation for financial institutions, e.g. around appropriate risk management when using alternative identifiers.
- Finally, **the outcome** will be enhanced access to remittances in a risk-controlled way.

Based on the goal, outcome and outputs as defined, the M&E framework then will provide appropriate key performance indicators (KPIs). KPIs should look at effectiveness and outcomes of the regulation and always be linked to ML-TF-PF assessment objectives as well as national development objectives such as financial inclusion, SDGs, among others. Examples of KPIs include the level of informalization in a country (as high levels of informalization could indicate the creation of an opaque financial market which increases risks), the appropriateness of compliance measures compared to the outcome in the industry, and the cost of compliance across the industry. This will be informed by the data collected, which is further discussed in Step 2 below.

Remember, any regulation without a measurable success indicator will likely not serve its purpose. You cannot regulate something if you do not know what the desired outcome is.

Step 2: Determine data sources for measurement of progress.[71] Building an empirical evidence base is an essential part of measuring whether you have met your KPIs and objectives. Data sources to draw on should be internal and external. Examples of **internal** data sources include data collected from financial institutions' risk assessments, the number of AML/CFT offences investigated and prosecuted, or the number and categories of suspicious transaction reports submitted.[72] Examples of **external** data sources to complement financial institution data include trade-based money laundering data, information on corruption and databases which highlight "bad actors" globally. Such databases can enable regulators to identify touchpoints of these "bad actors" in their financial system and use it to detect money laundering and tip off financial institutions. A key focus for regulations should be to regularly take stock of the available data in the industry or globally that could be utilized to better understand ML/TF/PF and similar threats facing the country and how to mitigate these. Regulators can enhance measurement of progress over time based on the availability of analytics, for example, they can start with a limited number of available datapoints and expand the framework to multiple datapoints once more data becomes available.

[71] Note: this step is not a static process. As you get access to more data, you will be able to target outcomes to be measured more clearly.

[72] Note that analysis of these simple indicators can be done by institution, but comparisons across the industry to identify patterns have to take place at the central bank level, as individual financial institutions do not have the sophisticated systems or oversight to monitor industry-wide financial activity.

Step 3: Dissemination. After assessing the extent to which your KPIs are being met, you should produce a report on the overall impact of the regulatory change and share it with the market for feedback. This may require regular meetings with the fora that you have engaged with throughout the process thus far. Such meetings provide an opportunity for continuous feedback and constant measurement. When receiving feedback, remember to reframe it in the scope of what you can address with the various legal instruments that are available to you, as outlined in table 3. Each type of instrument must remain within their bounds, for example, when more information is needed guidance can be provided but if it is a pervasive market or legal issue, the Act might need to be amended.

Step 4: Determine and implement remedial action. Based on the assessment of how KPIs have been met, a regulator will be able to establish the remaining gaps that need to be filled. In response, a corrective and remedial action plan needs to be formulated to address these gaps. Possible remedies include strengthening guidance, or changing the regulatory supervision roster or methodology, e.g. by having more on-site visits to those institutions who are unable to easily comply with the regulation. This relates to risk-based supervision and ensures that supervisory efforts are focused on the institutions that require it the most. Box 8 below provides a description of risk-based supervision. If the regulator finds that the regulation is not effective or not being followed by the industry, the first step should always be to increase engagement with the financial associations and the industry to better understand what needs to change to make the regulation more effective. It is also vital to maintain a community of practice, to ensure that institutions cooperate with each other and lead to broad industry-wide cooperation. Only as a last resort should fines or other punitive measures be considered.

BOX 8: What is risk-based supervision?

The risk-based approach was designed to make supervisors' efforts to detect and prevent the financial flows that enable money laundering and terrorism more effective (FATF, 2021). The risk-based supervision process is designed to consider the most critical risks facing a country's financial system. It also covers the assessment of the financial industry's management of these risks and potential adverse experiences. This process differs from compliance-focused processes, as it focuses on evaluating both present and future risks and effecting early preventative or corrective action moves (Deloitte, 2014).

Step 5: Recalibrate measures as needed. Once a defined period (typically one to two years, depending on the cyclical components of the intervention and measures) has lapsed, a final step is to revisit the measures of success and determine whether they require re-calibration. If none of the measures of success have been met, they may have been too ambitious, or ill-defined. This is a good opportunity to determine how to improve the indicators to measure progress more accurately or whether follow-up regulation or guidance is required.

5.4 Deep dive 4: A practical addition to the risk assessment intervention

SETTING UP A RISK ASSESSMENT MATRIX

Table 30 below **provides an example of how to set up a risk assessment matrix and illustrates how to complete the matrix** (that is, what kind of data and information to add). In the example, the RSP is assessing their product risk (which is one of the several risk types as explained above). The product attributes would be plotted in the rows, while the criterion for completion is in the columns. When implementing the example in your context, you will keep the criteria in the columns the same and change only the risk attributes in the rows to fit the risk factor that you are assessing (i.e. use risk factors that relate to your context). A few things to note:

- When completing this matrix, you will complete the same criteria fields as in the example.
- The table is followed by an overview of what each criterion on the columns means.
- It is essential to understand each of the fields and what information goes into each before you populate it with your data.
- The discussion below provides guidance on how to incorporate your data into the risk framework.

TABLE 30: **ILLUSTRATIVE EXAMPLE OF HOW TO SET UP A RISK ASSESSMENT MATRIX**

Objective: Assessing product risk (example)									
Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Column 9	Column 10
Product risk attribute	**Applicable or not in organization (Y/N)**	**Inherent risk classification**	**Inherent risk description**	**Weight**	**Risk mitigation mechanism**	**Control adequacy and effectiveness**	**Residual risk rating**	**Risk response**	**Risk assessment outcome**
Client type	Y	Lower	Non-verification of customer details	10 per cent	Effective verification system in place	Effective	Low	Tolerate	Risk mitigation is effective, therefore tolerate risk
Source of income or funds	Y	Medium	Customer may refuse to disclose correct source of funds	15 per cent	System will decline transaction that does not have source of funds	Effective	Low	Tolerate	Risk mitigation is effective, therefore tolerate risk
Local or cross border	Y	Medium	RSP has local and cross border transactions	10 per cent	RSP has proper system in place that detects where transaction is coming from and going to	Largely effective	Low	Tolerate	Risk mitigation is effective, therefore tolerate risk

Objective: Assessing product risk (example)

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Column 9	Column 10
Product risk attribute	**Applicable or not in organization (Y/N)**	**Inherent risk classification**	**Inherent risk description**	**Weight**	**Risk mitigation mechanism**	**Control adequacy and effectiveness**	**Residual risk rating**	**Risk response**	**Risk assessment outcome**
Financial sanctions	Y	Medium	Client name matches that of a sanctions list	8 per cent	Proper reporting procedure in place	Effective	Low	Tolerate	Risk mitigation is effective, therefore tolerate risk
Potential match with negative/ PEP list	Y	High	RSP may engage a PEP; RSP may also be unable to screen customers against all types of lists	8 per cent	Current screening process ineffective. RSP considering their own sanction screening solution.	Ineffective	High	Treat	Screening to be implemented and false positive rate to be determined
Occupation	Y	Medium	Customer may not give correct details about occupation	15 per cent	Information obtained from CDD process to control risk	Partially effective	Lower	Tolerate	Risk mitigation is partially effective, and overall risk remains low, therefore tolerate risk
High volume/ multiple transactions	Y	Low	Multiple transactions recently happening on RSP network	10 per cent	CDD process addresses this risk	Largely effective	Lower	Tolerate	Risk mitigation is effective, therefore tolerate risk
CDD/ECDD	Y	High	If CDD processes are not followed, there is possibility of paying a fraudulent transaction	18 per cent	Independent verification of IDs and validation of supporting documents	Largely effective	Low	Tolerate	Risk mitigation is effective, therefore tolerate risk
Remittance sending/ receiving corridor	Y	Medium	Most RSP corridors are not considered too risky; Will require data to determine risk of each corridor	6 per cent	CDD processes are followed. Ensure that funds are not coming from high-risk countries	Partially effective	Medium	Treat	Review data to determine country by country risk rating

Guide and key:

- The risk factor is filled into column 1 in row two (the block in blue), this is where you would add the factor you are assessing. For more factors, refer to table 31.
- The relevant risk attributes are listed underneath the risk factor, alongside the y-axis.
- The criteria according to which risk is quantified and the specific mitigants of each of the material risk attributes are assessed and formulated alongside the risk factor on the x-axis. These criteria are set and should remain the same regardless of the risk factor(s) and -attributes being assessed and regardless of the objective set. There is no need for you to change anything in this section.
- The information in this table is merely an example from a hypothetical RSP. You would need to insert your own information based on your data and circumstances. The section below this table provides an overview of what each criterion means, based on the column in which it is discussed, and it provides guidance on how to import your own data and information.

Column 1: Here you will list each of the **risk factors or risk drivers** for the component you want to assess, based on your organization's context. For examples of other risk factors to review, refer to table 31 below. The example above is for product risk; however, this same approach can be applied to various other risk factors. Note that each risk factor has its relevant risk attributes, which will be important to consider when designing risk mitigations as in column 6.

TABLE 31: **DESCRIPTION OF RISK FACTORS**

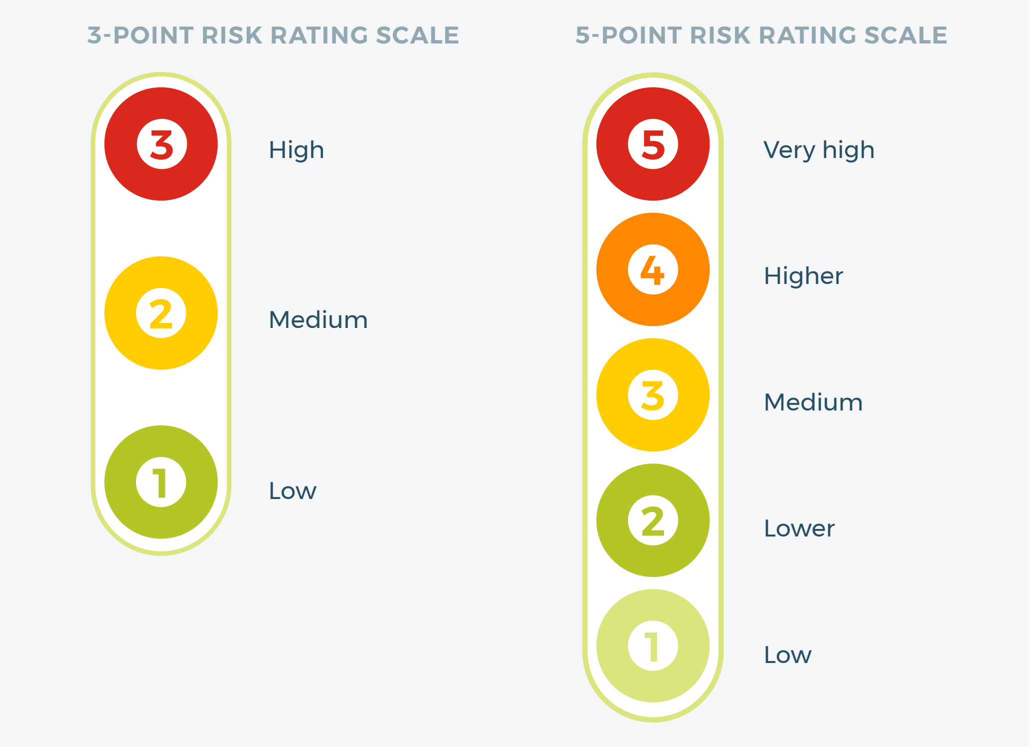
Risk factors	Description
Product risk	These are the types and attributes of the goods and services (such as confidentiality, transaction volume and speed, contract duration, etc.). Understanding the entity's risk profile also heavily depends on the profits from these (FATF, 2021)
Delivery channel risk	Refers to the characteristics of the delivery channels that are employed, which could include: the capacity to accurately identify and validate clients via digital or remote onboarding; the exclusive delivery of goods or services via mail, phone, internet, etc.; or the employment of introducers or intermediaries (and the nature of their relationship with the entity) (FATF, 2021)
Agent network risk	Agent network risk refers to the potential challenges and uncertainties associated with the use of agent networks instead of traditional branches to expand outreach and reduce costs. These agent networks, whether established through existing distribution channels like post offices and retail chains or through independent small-scale traders and retailers, play a crucial role in facilitating basic financial transactions on behalf of financial institutions and RSPs (CGAP, n.d.)
Client risk	Client risk is described as extra variables, like demographics and specialized offerings in terms of products and services for particular clientele groups; these include distinctions between natural or legal persons and those representing legal arrangements, the kinds of businesses that are served, the nationality or foreignness of the clients and the existence of any particular customer categories (e.g., Politically Exposed Persons) (FATF, 2021)
Regulatory and governance risk	A framework employed by entities to organize governance, risk management and regulatory compliance. The idea is to bring together and harmonize an organization's strategy for managing risks and sticking to regulatory requirements (Diligent, 2023)
Partner risk (also IMTO partnership)	Refers to the risks an RSP faces when partnering with an IMTO to process or pay out remittance transactions (52 Risks, 2020)
Technology risk	Refers to the adopting of new technologies which carry risks such as the potential exacerbation of cyber-related risks (by elevating the severity of cyberattacks or operational failures relative to traditional procedures), an excessive dependence on tech-models and reputational risks (if inaccurate algorithms are entered into technological applications, leading to incorrect supervisory assessments and actions) (FATF, 2021)
Geography risk	Regarded as the extent of the entity's domestic and international operations, encompassing the locations of clients, residences of beneficial owners and the receipt and transfer of funds, as well as the markets it serves; the strength of the foreign AML/CFT legal framework in which it functions; and contextual factors (such as levels of crime, terrorism, or corruption) and how those might impact the entity's strategy, especially with regard to online service providers, financial institutions, or other groups (FATF, 2021)

Risk factors	Description
Other relevant factors per jurisdiction	After reviewing all other risk factors, the last step is to consider any risks specific to your jurisdiction, location, region, or any other unique context. These risks include among others corruption, environmental risks, or even trade-related risks. It is vital to understand the risk factors or elements in relation to what is considered as the normal activity and predictable cycles for the country and region and what is an abnormal anomaly. The latter can be identified by reviewing data to identify patterns. Examples include exceptional values, changed distribution patterns, activity levels during festival periods or at the start of the education semester and abnormal activity coinciding with large irregular procurement contracts, prosecutions and elections.

- **Column 2:** This entails providing a **yes or no of whether the risk attribute is applicable** in your organization. This column serves as a completeness check or record of each component or risk attribute that was assessed and what was not. Although it has a binary outcome (yes or no), the record or description should indicate why it was or was not worth considering under this specific assessment. For example, if you include an attribute which is not applicable for the specific assessment, it should have a "No" outcome in column 2 accompanied by a note such as "no material risk level detected" or "no empirical evidence to date", etc. By recording this outcome, it gives your organization and the regulator an indication of how risks facing your remittance business have evolved over time.

- **Column 3:** This column is for you to add in the **inherent risk classification** for each attribute. This should be an indication of the rating or extent of risk. To do so, it's best to use a rating scale. The two most popular options for rating scales are a 3-point rating scale and a 5-point rating scale. While the 3-point scale is more popular, it does not allow for a granular assessment and understanding of risk attributes and can therefore lead to significant risk assessment errors when compared to the 5-point rating scale. The 5-point scale allows you to assess the impact more accurately and the severity of a risk. The scales are illustrated below:

FIGURE 9: RISK RATING SCALE COMPARISON



- **Column 4:** Describe the **key features of each of the risk attributes** here. This is also where you should incorporate data to provide additional evidence of how the attribute presents itself within your context. For example, *nationality risk* will be rated as medium to high if the RSP does not have the nationality of the sender, meaning that this data is not analysed. This presents a risk as there is limited insight into this potential risk due to no data.
- **Column 5:** Assign a **weighting to each risk attribute** based on its relative importance within your organization, its likelihood and history of occurrence.[73] The weights in the table are for illustrative purposes only and should be customized to your institutional context, be credible and stand scrutiny by your board, regulators and mutual evaluators as may be applicable. Note that all the weightings should always add up to 100 per cent.
- **Column 6:** Describe **key risk mitigation features** for each risk attribute, that is, key features that are relevant in determining residual risk. For example, you can do transaction monitoring and implement a screening system to flag when nationals from non-regular countries are sending or receiving money via your institution. This also includes screening for politically exposed persons (PEPs) and against top sanction lists, such

[73] These weightings should be based on empirical and historical data and should be informed by how your product interacts in your context and the national risk context. E.g. if a risk is very prevalent in your context and not as applicable in the national context, it should still receive a high weighting in your risk assessment. These weightings should also take the specific product context into account, e.g., if remittances are used for building homes, they will usually have large values. This should be picked up via frequent transaction monitoring and should therefore be rated proportional to the real risks posed to your organisation.

as the United Nations' Security Council lists, OFAC lists such as Specially Designated Nationals (SDN) list.[74] Here, you will also need to ensure that the mitigation strategies you adopt are effective in addressing drivers, as well as sub-drivers of risk and that they do not counteract each other.

- **Column 7:** Here you will indicate how **effective your mitigation strategy** is.[75] A 4-point rating scale is shown in **TABLE 32** below. This scale is typically used to avoid median tendency and encourage your organization to clearly decide whether the mitigant works, and if so, how well it works. Any measures should again be set based on empirical evidence, which needs to be tracked over a reasonable amount of time, we recommend 1–5 years. This approach allows you to view the overall impact of isolated incidents and provides an accurate depiction of the how each incident affects the overall risk assessment, and how it fits in with your product and market proposition, sustainability plans and KPIs. Importantly, any changes in your criteria or key indicators, like suspicious transactions, should also be considered. This will enable you to arrive at the most accurate determination of the efficiency of the controls you wish to implement and prevent any knee-jerk changes to the broader market proposition, for example redlining certain countries due to a handful of STRs. The outcome of this check will determine the residual risk rating in column 8 below.

TABLE 32: RATING SCALE FOR EFFICIENCY OF MITIGATION STRATEGY

Rating	Description
Effective	Control mitigates the full extent of the risk
Largely effective	Control mitigates the risk to a greater extent and less/some of the risk remains unmitigated
Partially effective	Control mitigates risk to a lesser extent and much/most of the risk remains unmitigated
Ineffective	Control does not mitigate the risk and the full risk remains unmitigated

- **Column 8:** The **residual risk rating** is determined as the portion of the inherent risk that remains after mitigation controls have been put in place. This risk follows the same rating scale as for the inherent risk.
- **Column 9:** Based on the residual risk rating in column 8, you will determine your **risk response**. This refers to how your organization will react to the risk that remains after controls have been implemented. Options include that you can treat or reduce the risk (applying controls and monitoring the controls), accept the risk (and do nothing), transfer the risk (e.g. to

[74] Other lists include the US based lists, EU lists, other OFAC lists such as Foreign Sanctions Evaders list, Non SDN Iranian Sanctions, Sectoral Sanctions Identifications, Non SDN Palestinian Legislative Council list, among others. In addition, there are supplementary and commercial lists that complement the above-mentioned international ones. These supplementary lists vary with jurisdiction and institutions. It may also involve internal list of blacklisted clients or offboarded clients, among other considerations.

[75] Another short-hand view of measuring efficiency is to determine whether the mitigation 1) is effective in terms of mitigating impact/size of the incidence of the risk and 2) is effective in terms of increasing the potential business (geographical) footprint of the organisation.

a third party who can manage it better), or avoid the risk (by de-risking and terminating certain customers, jurisdictions or products generating the risk), diversify (by focusing or getting into lower risk areas) or risk provisioning in the balance sheet to prepare for risks that materialize.

- **Column 10:** Finally, in the last column you will justify your risk response and write up the **outcome of the risk assessment** for that attribute. This can include that the risk is within our outside of your risk appetite, or which controls you wish to implement in future to further mitigate the risk.

Your next step is to incorporate your own data into the risk matrix. Please see box 3: A guide – how to incorporate data into your risk assessment in the main text for guidance.

5.5 Appendix accompanying chapter 2

TABLE 33: **OVERVIEW OF LEGAL INSTRUMENTS**

Regulation	Description	Relevant issuing authority
Act	A statute or act is a piece of legislation or decree, usually passed by a national legislative body having the force of law. Statutes, decrees, or laws need to be public documents and hence are usually published in formal government gazettes, bulletins or official journals or similar government publications. n.d.). Well-structured legislation addresses matters more at an enduring principle and framework level rather than practicalities and implementation details. For RSPs: these are the laws which form the structure and framework and broad scope within which you are required to act and comply with. If you do not act within the boundaries of the statue nor comply with the provisions, at a minimum, you are at risk of steps taken by the regulator, supervisor, or prosecutor. For financial sector regulators and supervisors: review laws to maintain the relevance of the framework of legal principles, prevent inconsistency with other legislation in alignment with market development requirements. Amendments approved by the legislature are adequately tested and socialized within industry and communicated to the public.	Central Bank Local government authorities Financial Intelligence Centre or Financial Information Processing Unit
Regulation	Regulation is delegated or subordinated legislation, meaning authority granted by legislation to create regulations that enable the implementation and functioning of the legislative framework. Regulatory authority is conventionally delegated to an executive role (e.g. a minister of a government department) or combination of executive roles on very specific topics. Regulation therefore should never exceed nor contradict the law from which it has been delegated and certainly never override the authority of the legislature. Ideally regulation should closely follow the structure of the law and provide the detailed instructions or modalities for implementation and smooth functioning of the legislation, only to the extent it is required. There are exceptions for instance in countries where regulations are issued as a legislative instrument, and which can technically have the same or greater force of law than the original statute. This is typically where there has been historically low trust between the legislature and the executive. Unless precisely formulated, regulatory instruments enacted by the legislature directly can be extremely nebulous for regulators and industry alike to navigate and effectively implement in comparison with regulation developed by regulators in relation to industry and promulgated by the requisite executive authority. The important points for RSPs, regulators and supervisor alike are to understand which is the most authoritative legislation and to map the legislative framework and then consider each regulation and how it modifies or directs behaviour within the legislative framework. Having a comprehensive map of the legislation and supporting regulations can provide a lot more clarity than reading anything in isolation. Legislatures can sometimes get it very wrong, but in general, law or statutes should tell you about the structure within which you may act, regulation should tell you how to act within that structure. For RSPs: ensure that you comply with these regulations. For regulators: review these regulations to prevent inconsistency and check for outdated documents being referenced.	Central Bank Finance Ministries Local government authorities
Guidance or Guidelines	Guidance documents, or guidelines, are authoritative statements issued by government agencies to inform the public of the policies or provide clarity on interpretation. The authority to issue guidelines, guidance documents, circulars and notices is contained within general legislation, organic laws or within specific legislation. They do not have same force and effect as laws but can be administratively persuasive. (United States Department of Justice, n.d.). For RSPs: ensure that you remain up to date with the most recent versions as these get published frequently. Re-evaluate your policies and processes including CDD and KYC in relation to the changes in guidance. For regulators: this is a powerful tool to provide guidance for the market on how to interpret or implement a piece of legislation. It is especially valuable in supporting and facilitating innovation, for example: Guidance Note 7 on implementing the risk-based approach (FIC, 2017).	Central Bank Finance Ministries Regional central banks Local government authorities Financial Intelligence Unit or Financial Intelligence Centre

5.6 Appendix accompanying chapter 3.5

TABLE 34: EXAMPLE OF AGENT RISK ASSESSMENT

Objective: Determine the extent to which you can rely on agents to conduct third party due diligence on your behalf

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Column 9
Agent delivery channel risk attribute	**Applicable or not in organization (Y/N)**	**Inherent risk classification**	**Inherent risk description**	**Weight**	**Risk mitigation mechanism**	**Control adequacy and effectiveness**	**Residual risk rating**	**Risk response**
Agent location	*Y*	*Low*	*Location of the various agents on the territory - no security and political crisis at the moment*	*10 per cent*	*KYA control or inspection and agent filtering*	*Largely effective*	*Low*	*Mitigation is effective*
Customer anonymity	*Y*	*Medium*	*Impersonating a beneficiary client*	*15 per cent*	*Inspection at withdrawal; proper training of agents on fraud*	*Effective*	*Low*	*Mitigation is effective*
Agent impersonation	*Y*	*Medium*	*An agent shows up on the ground with a false identity*	*10 per cent*	*All transactions are unique and validated by receipt with transaction ID*	*Effective*	*Low*	*Mitigation is effective*
Poor training on detection and prevention of ML and fraud risks	*Y*	*Lower*	*Passing fraudulent transactions on the platform*	*5 per cent*	*Improved annual training on ML-TF and fraud risk*	*Partially effective*	*Lower*	*Mitigation is effective*
Agent liquidity	*Y*	*Medium*	*Lack of cash in the network of agents impacting the end customer*	*15 per cent*	*Increased liquidity at point of sale*	*Effective*	*Lower*	*Mitigation is effective*
Agents deceiving customers	*Y*	*Medium*	*Risk of overbilling with customers which pose a reputational risk*	*15 per cent*	*Raising customer awareness on prices of services and formal notice process for non-compliance with policy for agents*	*Partially effective*	*Lower*	*Mitigation is effective*
The know your agent policy is not based on a risk assessment	*Y*	*Higher*	*Non-compliance with regulatory requirements*	*25 per cent*	*Monitor regulatory developments; develop or update policy in line with regulation*	*Partially effective*	*Medium*	*Implementation of new agent onboarding policies; educate agents on changes in the policy*
Data and privacy breach	*Y*	*Lower*	*Data loss due to cyber attack*	*5 per cent*	*Enhance security of systems*	*Effective*	*Low*	*Mitigation is effective*

Guide and key:

- The risk factor is filled into column 1 in row two (the block in blue), this is where you would add the factor you are assessing. In this case, it is the agent delivery channel risk.
- The relevant risk attributes are listed underneath the risk factor, alongside the y-axis.
- The criteria according to which risk is quantified and the specific mitigants of each of the material risk attributes are assessed and formulated alongside the risk factor on the x-axis. These criteria are set and should remain the same regardless of the risk factor(s) and -attributes being assessed and regardless of the objective set. There is no need for you to change anything in this section.
- The information in italics is merely an example from a hypothetical RSP. This is where you would insert your own information. Refer to section 5.4.1 for an overview of what each criterion means, based on the column in which it is discussed. The discussion there also provides guidance on how to import your own data and information.

IFAD

International Fund for Agricultural Development
Financing Facility for Remittances
Via Paolo di Dono, 44 - 00142 Rome, Italy
Tel: +39 06 54591 - Fax: +39 06 5043463
Email: ifad@ifad.org
www.ifad.org

facebook.com/ifad
instagram.com/ifadnews
linkedin.com/company/ifad
twitter.com/ifad
youtube.com/user/ifadTV

May 2024

FFR DONORS

IFAD
Investing in rural people

LUXEMBOURG
AID & DEVELOPMENT

MINISTERIO
DE ASUNTOS EXTERIORES
Y DE COOPERACIÓN
cooperación española

Sweden
Sverige