The Model Policy Framework on Digital Retail Payments for Micro, Small and Medium-Sized Enterprises in COMESA

Towards Digital Financial Inclusion for MSMEs in the Region

CBC COMESA BUSINESS COUNCIL
Voice of the Private Sector in the Region
BUILDING REGIONAL GOING GLOBAL

DFI4SMEs
A CBC Digital Financial Inclusion Program

Funded by
Bill & Melinda Gates Foundation

COMESA MEMBER STATES

Burundi; Comoros; Democratic Republic of Congo; Djibouti; Egypt; Eritrea; Eswatini; Ethiopia; Kenya; Libya; Madagascar; Malawi; Mauritius; Rwanda; Seychelles; Somalia; Sudan; Tunisia; Uganda; Zambia; Zimbabwe.

DISCLAIMER

The designations employed and the presentation of material in this publication do not imply the expression of the Consultant's or CBC Secretariat's opinions concerning the legal status of any country, territory, city or area, or of its authorities or concerning the delimitation of its frontiers or boundaries. Although CBC has gone to great lengths to ascertain accuracy of the information in this report, it cannot guarantee that the information is complete and updated. Estimates have been used in certain instances when data was unavailable. CBC is therefore not liable for any opinions or information that is contained in this Report.

The Model Policy Framework on Digital Retail Payments for Micro, Small and Medium-Sized Enterprises in COMESA:
Towards Digital Financial Inclusion for MSMEs in the Region.

TEAM LEADER
Dr Jonathan Pinifolo

EDITORIAL TEAM
Mr. Gad Awuonda
Mr. George Omino
Mr. Stephen Mwaura
Mr. Dickson Poloji
Mr. Yoseph Wondimu
Ms. Marianne Nzioki
Mr. Hopewell Musundire

DESIGN & LAYOUT
Mr. Tinashe Kavumbura

PUBLISHED BY
Business Facilitation Unit,
COMESA Business Council

Acknowledgements

This report was developed under the COMESA Business Council's Digital Financial Inclusion for Micro, Small and Medium-Sized Enterprises Program. It presents a policy framework whose objective is the development of policy, legal and regulatory measures for implementation and regional harmonisation; establishment of institutional arrangements to support the implementation of the measures; and monitoring the implementation of these measures.

The overarching vision is to strengthen cross-border trade, regional market access and boost intraregional trade in COMESA and continentally.

We would like to thank the COMESA Committee of Experts on Finance and Monetary Affairs, as well as the COMESA Committee of Central Bank Governors for the review, additional input and adoption of the report.

The Bill and Melinda Gates Foundation (BMGF) supported the COMESA Business Council SME Digital Financial Inclusion Plan grant agreement. Special appreciation goes to Mrs. Dilwonberish Aberra of the BMGF for her continuous advisory support towards the Digital Financial Inclusion Programme for MSMEs.

The report was developed by Legis Policy Associates, supervised by Dr Jonathan Pinifolo, the Digital Financial Inclusion Manager, under the overall supervision of the CEO, Ms. Sandra Uwera.

We further acknowledge the input by CBC's team of experts, Mr. Dickson Poloji, Business Policy Programs Manager; Mr. Yoseph Wondimu, Digital Services Operations Manager; Ms. Marianne Nzioki, Marketing and External Relations Officer; and Mr. Hopewell Musundire, Business Development Officer. Appreciation also goes to our partners Glenbrook - Ms. Elizabeth McQuerry, and AfricaNenda - Dr Robert Ochola, CEO; Mr. Goodluck Akinwale, Deputy CEO; and Mr. Michael Mbuthia, East Africa Regional Director.

Our special gratitude correspondingly goes to the following organisations constituting our Advisory Committee, for their support in the development of the report: Bayer Crop Science, KCB Bank Rwanda Plc, Vodacom, COMESA Clearing House, Techno Brain, Coca Cola East and Central Africa Franchise, ECOCASH, Airtel, GSMA, Bank of Zambia, Rwanda Information Society Authority (RISA), Kenya Bankers Association, and Bankers Association of Zambia.

Lastly, we would like to thank participants in our first and second High-level Public-Private Dialogues held on 20th January 2021, and 27th July 2021 respectively, who validated and adopted this report. They represented the nine pilot-study countries: Egypt, Ethiopia, Kenya, Malawi, Mauritius, Rwanda, Tanzania, Uganda, and Zambia. Participants in these countries were drawn from MSME Associations, Mobile Network Operators, Financial Services Regulators, Information and Communication Technologies (ICT) Regulators, FinTechs, and Agroindustry/Manufacturers.

Contents

Acronyms & Abbreviations

ACHS	-	Automated Clearing Houses
AML	-	Anti-Money laundering
API	-	Application Programming Interface
ATM	-	Asynchronous Transfer Mode
B2B	-	Business to Business
B2C	-	Business to Customer
BIS	-	Bank for International Settlement
C2C	-	Customer to Customer
CBC	-	COMESA Business Council
CDD	-	Customer Due Diligence
CFT	-	Combating Financing of Terrorism
COMESA	-	Common Market for Eastern and Southern Africa
CSRF	-	Cross Site Request Forgery
DFI	-	Digital Financial Inclusion
DFS	-	Digital Financial Services
DFSPs	-	Digital Financial Services Providers (DFSPs)
DOS	-	Denial of Services
DRP	-	Disaster Recovery Plan
EAPS	-	East Africa Payment Scheme
EMV	-	Europay, Mastercard and Visa
ESAAMLG	-	Eastern and Southern Africa Anti-Money Laundering Group
FATF	-	Financial Action Task Forces
FMI	-	Financial Market Infrastructure
FMIS	-	Financial Management Information System
FSPs	-	Financial Service Providers
GDPR	-	General Data Protection Regulation
GPS	-	Global Positioning System
ICT	-	Information, communication and Technology
ID	-	Identity
ITU	-	International Telecommunication Union
KPI	-	Key Performance Indicators
KYC	-	Know your Customer
MDA	-	Ministries, Department and Agencies
MMO	-	Mobile Money Operator
MOU	-	Memorandum of Understanding
MSMEs	-	Micro, Small and Medium Enterprises
NFC	-	Near Field Communication

NGO	-	Non-Governmental Organization
OECD	-	Organization for Economic Co-operation and Development
OPEX	-	Operational Expenditure
PSPs	-	Payment Services Providers
QR	-	Quick Response
RECs	-	Regional Economic Communities
RTGS	-	Real Time Gross Settlement
RTP	-	Real Time Payment
SADC	-	Southern Africa Development Community
SIRESS	-	SADC Integrated Regional Electronic Settlement System
SPV	-	Special Purpose Vehicle
SQL	-	Structured Query Language
SWIFT	-	Society for worldwide Interbank Financial Telecommunication
UPI	-	Universal Payment Interface
URL	-	Direct Uniform Resources Locator
VAS	-	Value Added Services
VPAS	-	Virtual Payment Addresses
XSS	-	Cross Site Scripting

Executive Summary

This digital retail payment platform has been developed based on the following premises: there being a commercial rationale for a critical mass of Member States to move towards creating an interoperable payments system; and a public policy to enforce this action.

The Common Market for Eastern and Southern Africa (COMESA) region has various national digital payment policies and frameworks that need harmonization. The policy work will begin with the streamlining of individual policies with the model framework. COMESA Member States will converge their individual policies into a common set of integrated digital real-time retail payments policies, which respond to and address the challenges associated with Digital Financial Inclusion (DFI). This digital retail payment platform has been developed based on the following premises: there being a commercial rationale for a critical mass of Member States to move towards creating an interoperable payments system; and a public policy to enforce this action. The Policy needs to provide an over-arching framework based on a coherent approach to coordinate the multiple actors, who are involved in the payment system. It should also provide the basis for developing regulation and other government interventions.

The recommendations from the business case report were strongly in favor of the need to strengthen policy environment, within which the implementation of digital low-value or retail payments will be done. The current absence of an overarching policy framework on key elements of retail payments creates uncertainty and undermines the case for decisive action and investment. Therefore, the Member States will prioritize the development of the policy and regulatory framework for retail payments alongside a roadmap for its implementation. The objectives of the policy framework are the: development of policy, legal and regulatory measures for implementation and/or regional harmonisation; establishment of institutional arrangements to support the implementation of the measures; and monitoring the implementation of these measures.

Four key pillars namely; legal and regulatory framework; infrastructure; incentives for use and access; and capacity building, support and are required to achieve the vision and objectives of the policy framework.

Four key pillars namely: legal and regulatory framework; infrastructure; incentives for use and access; and capacity building, support and are required to achieve the vision and objectives of the policy framework.

These pillars are expected to address the existing national policy frameworks that need: regional harmonization and standardization; the dominance of cash payments due to lack of interoperable infrastructure; gaps in the payments and network infrastructure across the COMESA region; multiplicity of regional payment systems in COMESA region; and lack of a single digital platform to enable Micro, Small and Medium Enterprises (MSME) domestic and cross-border business transactions and payments.

The framework proposes the implementation of various policy, legal and regulatory measures in a bid to enhance DFI. Additionally, it calls for the harmonization of eight key policy areas towards attaining the same objective, including: cyber security; consumer protection; Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT); electronic transactions; and data privacy and protection. Additionally, four policy areas in the Information, Communication and Technology (ICT) infrastructure across markets need to be harmonized namely: Infrastructure Sharing Policy, Administrative Incentive Spectrum Pricing Policy, Quality of Service guidelines; and Universal ICT Access Policy.

The policy framework has also set out institutional arrangements to facilitate its implementation. This takes into account factors that will expedite the development and implementation of the regional digital retail payments platform for MSMEs in COMESA. Similarly, the framework provides an implementation matrix that outlines the: activities; policy, legal and regulatory measures; and entities that are responsible for, or will be involved in the policy implementation. This is a model policy, which will facilitate the development and implementation of a digital retail payments platform within and across COMESA Member States. These will either leveraging on or complement the existing regional payments platforms.

1 Background

Expanding intra-Africa trade is crucial to fast-tracking economic growth on the continent. This is one of the primary objectives of the Regional Economic Communities (RECs) such as the COMESA.

Expanding intra-Africa trade is crucial to fast-tracking economic growth on the continent. This is one of the primary objectives of the Regional Economic Communities (RECs) such as the COMESA. Intra-regional trade is important for Africa's many small, landlocked countries that face challenges while trading internationally. But, the internal trade in Africa is low, accounting for about 10 percent of its total trade. For Instance, in 2019, intra-COMESA's total exports and imports stood at US$ 10.9 billion and US$ 11.2 billion, respectively. It is therefore important to increase intra COMESA trade in order to give more opportunities for businesses and the population. There is a need to start a reliable digital payment infrastructure in the region, to maximize on the benefits of intra-COMESA trade and increase transactions.

COMESA's formal financial services/product providers still exclude a significant proportion of the population and small businesses in the region. Some of these small businesses only use their bank accounts for basic services (under-banked) because they lack access to finances from formal financial institutions and Value-Added Services (VAS). It is important to note that access to formal payment channels and services can offer a pathway to access to a wide range of financial services, which highlights the importance of financial inclusion of MSMEs. DFI is one channel through which ICT can ease both intra-regional trade and economic growth. Developments in ICT including mobile telephone subscriptions, allow the expansion and access to financial services for MSMEs in remote areas of the countries. This can result in increased remittances and regional trade at a very low cost within a permeating distribution network. Such initiatives can help deepen financial inclusion and reduce transaction costs across the COMESA region, thus increasing intra-regional trade.

Digital payments still account for a small percentage of the total payments and settlements transacted by MSMEs in most COMESA Member States. Cash remains the most common form of payment especially for national and cross-border retail transactions in the region. The migration from cash to digital forms of money is still far from completion, although the process being already underway. The impact of transaction costs related to the payment systems is usually significant in relation to the relatively small-size of transactions in which low-income households and MSMEs are engaged. Viewed from the customers' perspective, these transaction costs include the overall cost of accessing the digital retail payment systems, among others. Physical access to payments' infrastructure is especially pertinent in rural areas that often have limited footprints of Payments Service Providers (PSPs). In terms of the supply-side, their ability to enter the market even for small-time suppliers, has profound implications on the effectiveness of market functions.

Mobile money has shown myriad applications of a low-value payments solution, which allows value to be transferred across space. This has driven revolution in the retail markets in countries such as Kenya and Uganda, which has provided a near universal solution, connecting consumers, business and government. This success can therefore be used to create an open payments infrastructure, which promises to provide a basis for further deepening of financial inclusion, and to enhance economic participation. The region has made significant progress in laying down the foundations for mobile money transactions.

There is firm agreement on the idea of developing a digital retail payments system. However emphasis should be put into the creation of incentives, which will ensure the adoption and utilization of the system once it is developed. Payments are aimed at facilitating the transfer of value between individuals and enterprises for economic resilience and growth. The flow of money both cheaply and seamlessly through the payments' infrastructure should be a fundamental policy priority. Case in point India, whose sole purpose is to create a low-cost, fully interconnected network that works for all.

The State considers its role as that of creating the public goods that are necessary for the utility to flourish for the common good, as opposed to the ownership and operation of the utility. They have based their approach on two key concepts, thus the: promotion of interoperability at all levels of the value chain; and direct provision of certain technical standards, and shared service elements by public entities.

The COMESA region has experienced success through: the widespread adoption of mobile phones within the population; strong action and large investments by certain large private market players; and an enabling regulatory stance that supported market participants to experiment, and later scale-up their operations. But despite the early success, there are some signs of the journey being incomplete and, in fact, may be more fragile than it seems. The following are some reasons that have been advanced for this:

- Most accounts have little or no value: Although services such as digital saving encourage people to use digital instruments in their daily transactions, many accounts have little or no value in them. A majority of the people use payment instruments as a means of making payments, but not much as a store of value. Most transactions start and end in cash, which means that while payments are being digitized, cash is not. This limits the potential of taking digital payments into daily transactions, because people have a natural preference for making cash payments.

- Limited use of mobile money among formal businesses: Most formal businesses continue operating largely using cash. Mobile money is increasingly being used to collect funds from customers under a bill pay service, or to pay wages under a bulk pay service. But, very few businesses have re-engineered their business to be cash-free in an effort to exploit the fact that practically all their customers, employees, suppliers and business partners are connected to mobile money networks. In addition to this, the current mobile money systems lack the manageability and reconciliation tools that most businesses need.
- The cost remains high: Retail payments are a volume business. With the explosive growth in mobile money transactions that have been witnessed over the years, one could have wished to see the per-transaction costs reduce at a faster pace. From the customer's perspective, pricing is very attractive relative to alternatives for remote payments, but less so for proximity payments, where cash remains a better option. Lower prices across board would help speed up transition to a cash-lite environment.
- Some basic trust issues still need to be resolved: Although service reliability and uptime have improved over the past few years, they are still a major a sticking point for customers who depend on mobile money for their businesses and lives. The explosion of mobile-based lotteries and credit may pollute perceptions around the safety of mobile money more generally, if they have hurt a substantial number of customers. It may be necessary to establish additional basic consumer protection rules and practices around such services.
- Lack of awareness and knowledge regarding the benefits of Digital Financial Services (DFS).

However, if the real potential is to be achieved, the level of ambition and pace of change must increase. The payments' system needs to be developed to create a digital money 'grid' or utility which is:

- Inclusive: connecting all individuals as a basic factor of modern citizenry;
- Unrestricted: allowing all people and businesses to either send or receive money to/from anyone using various payment instruments and channels;
- Inexpensive: providing a viable low-cost solution for all payment types and values;
- Prolific: offering a wide range of payment and other financial services; and
- Diverse: encouraging a diverse range of players to emerge, innovate, and compete effectively.

The COMESA Business Council's (CBC) Digital Financial Inclusion Program for MSMEs, seeks to harness the potential of digital technology and establish an integrated low-value retail payments platform. It is expected that the participation of MSMEs will drive up regional trade, while increasing the volumes of cross-border transactions. The realization of this objective calls for the development of a policy framework that will set the foundation for the establishment of the regional digital payments platform. The wider goals for the payments platform should go beyond developing retail payments and facilitating trade, to enhancing greater DFI for MSMEs. The successful development and roll-out of the COMESA digital retail payment platform requires a supportive policy framework, existence of strong payments infrastructure, wide acceptability of different payment methods, high connectivity levels, public-private stakeholder commitments and collaboration, and the preparedness of different Member States.

The policy seeks to directly support the creation of the single most important piece of infrastructure in the finance industry - an open system that will minimize frictions related to money transfer across the region. This will increase competition and lower costs across the system, thus enabling expansion in the range and value of solutions offered.

A comprehensive, economy-wide approach is required if these objectives are to be achieved. There are various on-going initiatives within the Member States and regional economic blocs, which are aimed at enhancing the payment systems in the respective countries and regions. If the objectives of this policy are to be achieved, these initiatives will need to not only driven considerably further, but also harmonized to establish a stepwise efficient outcome. This must be backed by willingness of the Member States to collaborate, for the greater good of the COMESA region. Similar levels of collaboration are required amongst the various regulatory bodies, notably the Central Banks and payment regulators.

The policy will consider common core payments infrastructure that:

- Supports Real Time Payments (Universal Payments or Instant Payments)
- Integrates all channels (Omni-Channel)
- Is available, accessible, affordable and interoperable

It is important to note that the policy is aligned to the COMESA MSME Policy and Implementation Strategy that was adopted by Member States in October 2013, specifically on Implementation Result Area 5.4 - Improved Enabling Environment for Growth.

1.1 Vision

To have an enabling policy environment for financial inclusion of MSMEs for competitive delivery of innovative, real time, convenient, safe, and affordable digital payment solutions.

1.2 Objectives

The policy framework has the following objectives:

- To provide policy, legal and regulatory measures that will support the development of a regulatory environment, which can host a regional digital retail payment platform;
- To set up national and regional institutional arrangements that support the implementation of the policy framework.
- To monitor the implementation of the policy framework.

1.3 Guiding Principles for the Policy

The policy on digital retail payment platform will be supported by the following key principles and features:

Real-Time

The system should have the capacity to make real-time payments and same-day settlements towards ensuring that they meet the MSMEs' liquidity needs. The settlement rules should be harmonized across Member States. During the harmonization process, it will be important to consider the fact that different Member States have different transaction limits, which could affect the settlement amounts for individual accounts.

Irrevocability

Payments should be irrevocable as a key enabler for building trust in the system, especially for cross-border payments harmonized irrevocability rules and regulations should emphasize on the same across Member States. There will be a separate but complementary mechanism for handling payment reversals, in the case of wrong payment addresses.

Identity

A strong identity and electronic-Know Your Customer (e-KYC) framework linking the payer and payees to the national identification databases and system should be emphasized. This should include the infrastructure for addressing payments including bank accounts, mobile phone numbers, and authentication frameworks, such as biometrics that are stored securely. There should be a robust mechanism that differentiates the mobile and account numbers of participating Member States.

Open and Interoperable System

The platform should include both banks and non-bank Digital Financial Services Providers (DFSPs) who are eligible as direct participants in the scheme.

Equivalence of Transactions

Cross-border payments should be indistinguishable from domestic payments; similar rails should process both large and small value payments with none prioritized over the other (value-agnostic); and the underlying infrastructure should be common for all payments, especially Real Time Payments adopted by most jurisdictions. In terms of settlement currency, the platform will be multicurrency. During the agreed upon time that shall be stipulated in the rules, the Switch should determine the net position in local currency. The Switch will then send credit or debit settlement instructions to the Central Banks' Real-Time Gross Settlement (RTGS), which will then either debit or credit the pre-funded accounts. A list of supported settlement currencies including a mechanism accompanying it in the case of a different currency shall be availed.

Digital Financial Inclusion

This will help MSMEs in marketing their products and undertaking cross border transactions, thus facilitating their participation in regional trade.

2

Key Pillars of the Policy Framework

Different countries within the COMESA region are at different levels of development in relation to their operational, legislative and policy frameworks in the payment systems. Agreeing on a broad and comprehensive strategy will also allow key operational questions to be addressed.

Different countries within the COMESA region are at different levels of development in relation to their operational, legislative and policy frameworks in the payment systems. However, most of these countries have put in place supporting legal instruments for payment systems, which tend to be aligned to national, as opposed to regional payment objectives. This highlights the importance of implementing a regional framework that will support a regional MSMEs digital retail payment platform.

The successful development and roll-out of the COMESA digital retail payment scheme requires: a clear policy, legal and regulatory framework, existence of robust payment infrastructure; the ability to use and access payment platforms; a high degree of connectivity; and readiness of different Member States. A strong central leadership is critical in championing the agenda, and pulling together all these elements in a coherent manner. While a majority of the Member States have already put into place a number of the supporting factors, others still need significant effort, time and financial resources. The existing payments systems include: COMESA's Regional Payment and Settlement System (REPSS); Southern African Development Community's (SADC) Real-Time Gross Settlement (RTGS); East Africa Payment System (EAPS); Interbank Payment Systems Group of Central Africa (GIMAC); and the Electronic Banking Interbank Grouping of the West African Economic and Monetary Union (GIM-UEMOA) among others. At the same time, policy leaders in most Member States' are committed to having electronic payments forms within relatively short periods.

However, the region does not have a comprehensive policy and strategy towards digital payments, encompassing the different forms of payments taking place in isolated places. The impact on efficiency, cost, and wider public policy objectives depends centrally on the scope, besides the enabling digital payments to cover as many collection and payment points as possible. But, these must be carefully developed in a sequential and phased approach, starting with piloting on relatively easy payments, then rolling out to payments that are either high value, or small but high-volume transactions.

Agreeing on a broad and comprehensive strategy will also allow key operational questions to be addressed, including: what is the state of readiness of Member States and what kind of ICT and back-off capabilities do they need?; How will Member States drive DFI, and enable the excluded to access financial services including payments?; Who meets the infrastructural construction costs, and is there a role for public funding if positive externalities are possible?; and How do we leverage private sector solutions by enhancing integration of existing infrastructure, or encouraging development of new solutions, where the volumes of payments are large enough to give a commercial return, but with competitive and affordable pricing, or where diversity in payment solutions is needed for different contexts (small/large payments, or mobile/card/online payments)?

The following are the four key pillars that are required to ensure that the vision and objectives of the COMESA Digital Retail Payments Policy are achieved:

a) Legal and regulatory framework;
b) Technology infrastructure;
c) Incentives for use and access; and
d) Capacity building.

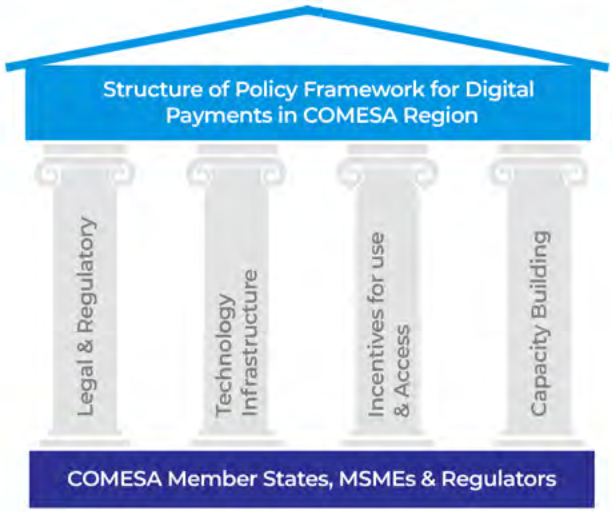


Figure 1: Structure of policy framework for digital payments in COMESA

Each pillar complements the other in supporting MSMEs in the COMESA Region. These four pillars will support the development and implementation of a sound policy framework, which provides a firm foundation towards ensuring that the digital retail payment platforms are responsive to the needs of MSMEs in the COMESA Region. A strong institutional framework will support the four pillars.

The pillars are expected to address the: existing national policy frameworks that need regional harmonization and standardization; dominance of cash as a means of payment; absence of interoperable infrastructure; gaps in the payments and network infrastructure across the COMESA region; and multiplicity of regional payment systems in COMESA. The promotion of a harmonized policy framework across Member States could result in increased efficiencies and hence lower operational costs to the Payment Service Providers (PSPs), and ultimately lead to a reduction in consumer costs.

Some of the policy, legal and regulatory gaps that were identified for purposes of developing a regional digital payment platform include:

- Security and consumer protection;
- Alignment of national and regional financial services regulations including money laundering, data privacy, Know Your Customer (KYC), among others;
- Inter-Bank Payment Compensation Rules;
- Routing rules;
- Regulatory and operational framework;
- Mobile money guidelines;
- Interoperability with various payment systems and distribution channels;
- Ease of access, especially to MSMEs;
- Clearing and settlement issues; and
- Exchange rates convertibility.

The issues have been examined below with the aim of coming up with policy, legal and regulatory measures to address them:

2.1 Legal and Regulatory framework for Digital Payment Platform

Legal and regulatory frameworks are at the epicenter of both regional and national payments and settlement schemes. Different countries within the COMESA region are at different levels of developing their payment system's operational, legislative and policy frameworks. A majority of the countries within the region already have the legislation and supporting regulations, and directives on payment systems. However, these are aligned to the national payment objectives as opposed to the regional aspects. Therefore, a harmonized legal and regulatory payments framework does not exist in the region. This highlights the importance of putting into place a legal and regulatory framework that will support a regional digital retail payment platform for MSMEs.

Public and Private sector collaboration is important in ensuring that the legal and regulatory framework remains adaptive, relevant and responsive. It will also bring together expertise and resources that are necessary in providing a good legal and regulatory environment.

The following are some of the key areas that are expected to strengthen the legal and regulatory framework for the MSMEs digital retail payments platform in COMESA region.

2.1.1 Cyber Security

The growth of ICT has revolutionized the conduct of business globally. However, the increased access to the internet has presented numerous risks and threats. Cyber-attacks are a looming threat to the payments industry. Despite the fact that cyber security is one of the most serious economic and national security challenges that is faced in the world, many governments are inadequately prepared to counter it. This is further complicated by the ever-evolving cyber security landscape. It is difficult to quantify the likelihood of a major vulnerability. The advent of potentially dangerous security weaknesses in the majority of computers as a result of errors in recent processor technology shows the degree of uncertainty. At the same time, the cybercrime landscape has evolved into a set of highly specialized criminal products and services that are able to target specific organizations. They do so by using a sophisticated set of malware exploits and anonymization systems, which routinely evade present-day security controls.

Cyber security vulnerabilities present a risk to the financial sector (systemic risk), and to individual financial institutions. Individual Financial Services Providers (FSPs) must safeguard and undertake a regular assessment of the cyber security of their services, and report the results to the supervisory authorities. The functionality of a payments system is segregated across multiple levels of operations. Hence threats to its security can also be segregated based on each level:

- Network level: Any security risk that is present in an underlying network infrastructure may compromise the payment system. Therefore, all devices and servers should be properly configured and the network perimeter protected against unauthorized access.
- Transaction level: At this level, the security concerns include the acceptance of an invalid transaction, such as zero or negative amount transaction, and/or transaction with invalid details. Hence, the validity of all transactions should be checked properly before they are processed.
- Application level: This level is concerned with the coding standard of payment gateway, and subject to the application security risks including: SQL injection; Cross site scripting (XSS); Direct Uniform resource locator (URL) Access; and Cross-Site Request Forgery (CSRF), among others.

As a result of the economic, social and political impact of a successful cyber-attack on a digital payments system, it is essential to further invest in security measures and disaster preparedness. The authorities in the Member States have the responsibility of setting up a national cyber security framework, defining and auditing the FSPs' obligations and cyber security readiness respectively, and providing coordination across the sector. As cyber threats transcend borders, there is also a need for regional co-ordination. Cyber security is a cross-cutting issue that applies to the entire region's infrastructure. Approaches to addressing cyber security must be cross-sectoral, and address all the nuances of the financial sector. In particular, they should deal with the vulnerabilities that arise from recent advances, such as mobile money, initiatives in financial inclusion, and FinTechs. For this reason, a harmonized cyber security framework, which specifically addresses the needs of the digital payments system, and the wider financial sector is required.

Proposed measures are that Member States should:

- Develop national cyber security policy frameworks, which are currently inexistent.
- Deploy an analytics-led approach to their existing fraud and crime monitoring and detection frameworks.
- Develop tailor-made continuous capacity building for security stakeholders to enable them better understand crimes related to payments.
- Have a structured way of knowledge/incident reporting and sharing. This will facilitate peer learning among entities and guarding against common crimes, while creating room for common responses.
- Develop cyber security frameworks that address the needs of digital payments.

2.1.2 Consumer protection

Recent developments, especially those enabled by technology, are bringing into the market a large number of consumers of new financial services. A majority of these consumers are more vulnerable to abusive practices, or the negative financial effects of inappropriate solutions. Member States have made significant strides in attaining a level playing ground in terms of financial inclusion and sophistication (partly driven by FinTechs and mobile). However, the wide range of issues that influence market conduct including the protection of customers, handling of complaints, disclosure, transparency, and financial education have not moved at the same pace. While this has resulted in a significant increase in financial inclusion, it has also exposed customers to equally significant risks including abuse.

Additionally, financial systems are developing at a fast pace. However, despite this, there is limited understanding of how to handle risks associated with FinTechs and innovation. The other difficulty is occasioned by how other allied issues such as the incorporation of market structure and competition integrate into broader financial regulation. The development of a harmonized consumer protection framework across Member States can help in the management of these elements. Implementation of a proper framework will help reduce harmful risk, while at the same time shaping incentives for providers to develop solutions that are beneficial to their clients in the long term. This is, therefore, a major priority area for the policy framework. The establishment of a supportive regulatory architecture is a crucial starting point in tackling all areas in the policy and regulatory system. While consumer protection is key, a majority of the sector regulators, such as Central Banks and payment regulators consider it as being secondary to their core concern over stability.

Given the impetus in integration and trade across the region, this framework can offer foundational knowledge and push for the strengthening of consumer protection oversight across the entire COMESA region. While bank accounts form the single largest share of financial system assets in the region, payments are becoming an integral part of the movement of value, in both large/corporate and retail, low-income market segments. The existing prudential guidelines on consumer protection should be reviewed, towards ensuring that they are up to date with current banking and payments practices. This assessment should include the incorporation of new tools and the provision of evidence on the design of various elements. The entire consumer protection agenda will need intense and target capacity strengthening for enforcement and coordination on topics, where multiple regulations have cross-jurisdictional mandate such as mobile, data protection, and consumer education.

Lastly, the emerging sophisticated use of digitally derived data has resulted in tremendous changes in financial inclusion. However, this carries significant risks to basic rights. A regulatory framework and industry standards, which will help clarify data ownership, ensure respect of right to privacy, and prevent potential abuses are needed.

Proposed Measures are that Member States should:

- Establish the data protection, security and privacy provisions that facilitate the efficient flow of remittance transactions.
- Develop and adopt a uniform COMESA digital financial consumer protection framework in line with the EU's General Data Protection Regulation (GDPR) framework, which is an acceptable global standard on consumer protection and data/information privacy.
- Support PSPs and payment intermediaries to implement regular and continuous consumer and user financial education programs, in consultation with financial sector regulators in order to increase digital financial literacy.
- Establish dispute resolution mechanisms to allow simple, low-cost ways of providing redress, and dealing with large numbers of uncomplicated retail problems without involving the court system.
- Develop and enforce cross-industry standards for addressing and resolving customer complaints on a timely and efficient basis, which are appropriate to the specific needs of customers and the delivery channel.
- Develop effective awareness programs to empower consumers.
- Cooperate in financial literacy/education programs through multi-stakeholder participation.

2.1.3 Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)

The effective AML/CFT are essential to the protection of the integrity of markets and the regional financial framework. This is because they help mitigate the factors that facilitate financial abuse. Money laundering and terrorism financing activities in one country can have serious implications across-borders and even globally. Jurisdictions with either weak or ineffective controls are especially attractive to money launderers and terrorism financiers.

Among the issues that should be included in the policy for digital payments are:

- International legal obligations of Member States;
- Anti-Money Laundering/CFT regulations issued by appropriate international regulatory bodies (Financial Action Task Force[FATF]);
- Member States to conform to standards set by international bodies on AML/CFT, such as FATF and surveillance by FATF styled regional bodies including ESAAMLG;
- Proportionate risk-based approach that provide flexible KYC/Customer Due Diligence (CDD) requirements based on the value of cross border transactions;
- International exchange of information; and
- Strengthen national laws dealing with illicit financial flows.

Proposed measures are that Member States:

- Without AML/CFT legislation to consider enacting them.
- Are urged to strengthen national legislations dealing with illicit financial flows.
- To consider increasing provision of financial integrity information and creating awareness on financial integrity to relevant stakeholders.

2.1.4 Electronic Transactions

The main purpose of payments is to facilitate the transfer of value between individuals and enterprises for economic resilience and growth. Thus, money flowing seamlessly through the payments infrastructure should be a fundamental policy priority for all governments. This approach is best exemplified in India, where the government's main objective is to create a functional low-cost, and fully interconnected network that benefits all citizens. The role of the state is considered to be that of creating public goods that are necessary for the utility to flourish for the common good, as opposed to its ownership and operation.

The country has based its approach on two key concepts: promotion of interoperability at every level of the value chain; and direct provision of certain technical standards, and shared service elements by public entities.

The COMESA region has achieved this through: the widespread adoption of mobile phones within the population; strong action and large investments by a cross-section of large private market players; and an enabling regulatory stance that has supported market participants to experiment, before implementing fully. But despite the early success, the journey is incomplete and could be more fragile than it appears.

2.1.4.1 Electronic Transactions Act

COMESA Member States individually and collectively agree to implement electronic transactions including National Digital Identification (e-IDs) and e-KYCs for all people and institutions that are integral to regional Real Time Payments (RTP). The policy will provide for a Unified Payments Interface (UPI), supported by standard Application Programming Interfaces (APIs), which will in turn support instant payments across the COMESA Region. Processes related to the e-ID and e-KYC need the personal identifier elements listed below as a minimum for every entity/person:

- Unique e-ID number for all citizens, MSMEs, companies, private institutions and Government/public entities (MDAs and NGOs);
- Link to Mobile Phone Number (primary phone number);
- Link to Bank Account Number (primary bank account);
- Biometrics including fingerprints, eye-iris scan, digitized picture, location/GPS data (Location data can enable APPs to flag or stop payment to a recipient in case the registered GPS/location data points to the “wrong” geographic location);
- Virtual Payment Addresses or Aliases (VPAs) that de-link a recipient’s primary bank account from his personal identifiers; and
- Virtual Payment Addresses or Aliases (VPAs) can include the recipient’s registered primary email address as their VPA accounts

The National e-ID Database Agency must always ensure that the personal identifiers of payers and payees are linked or mapped to the e-IDs, primary mobile number, primary bank account and biometrics to support authentication, identification and verification of e-ID, and performance of e-KYC processes. In the absence of a reliable means of identifying customers, digital payments will always be restricted in terms of what can be delivered to the Member States. Lack of a digital identity mechanism introduces friction into the financial sector which partly leads to high costs, slows down customer’s access to services, and reduces the range of services that could have been available to them. The first step in addressing this issue is for Member States to develop a harmonized infrastructure for biometric enabled national e-ID service, which people can use to authenticate their identity for both face to face and remote identity transactions. A national e-ID service that can be authenticated across Member States is of significant value to Financial Services Providers (FSPs).

This is because it allows them to both identify the person applying for the service, as well as giving them the confidence that they are serving the right person, in a process known as e-KYC.

This is a costly activity, and Member States should take advantage of technology in an effort to reduce these costs. In this case, it is possible for one financial institution in a Member State to complete the process, and then avail the results to others via a form of 'digital locker'. The contents are kept under the control of the customer and the originating FSP, in an approach known as shared KYC. The customer can then choose to make the contents available to other FSPs on a case-by-case basis, so that they can open accounts and offer other financial services seamlessly, without incurring the costs of repeating the customer on-boarding process. This process is undertaken on the basis that each FSP covers its own costs, rather than charging other FSPs to access the shared KYC resource.

The FSPs consider this to be most equitable and cost-effective way of attributing costs, since their size and on-boarding activity can be assumed to be broadly proportionate to the number of customers. .

Whereas shared KYC would appear to be a sensible approach to minimizing the industry-wide costs associated with customer on-boarding, there are issues that must be addressed before its widespread adoption, including: standardization (development and adoption of a standard approach, quality, etc); trust (that other FSPs are adhering to the agreed upon standards when carrying out the process); and liability. Additionally, in some cases, there are those individuals who lack documentation, and cannot be 'left behind' as a matter of policy, as the region moves towards a digital economy. Consideration should, therefore, be given to such cases to allow the adoption of an incremental model that gives everyone the opportunity to participate in the digital economy.

2.1.4.2 Electronic platforms and digital payments to comply with COMESA Member State's National Tax obligations and Customs laws

Electronic platforms and digital payment methods introduced new opportunities for producers especially for small and medium enterprises (SMEs) and start-ups. The digital economy and electronic payments have presented an opportunity to foster economic growth for both developed and developing countries. However, these could pose challenges for resource mobilization through the leakage of tax resources in developing countries, especially those in African. In order to promote the benefits of a digital payments platform and mitigate against the challenges of digital economy on the COMESA members states, the platform will comply with the Member States' constitutions, national laws, and national regulations. It will also conform to the international obligations, especially the national tax requirements, and customs, laws, and regulations. In addition, the proposed system will have to comply fully with the national trade systems and Member States' international trade regulations. It is important to note that the agreement that the Organization for Economic Co-operation and Development (OECD) and other international organizations endorsed as broad taxation principles at Ottawa in October 1998, should apply to e-commerce, thus:

a) Neutrality: taxation should seek to be neutral and equitable between forms of e-commerce, and conventional and e-commerce, thereby avoiding incidences of double taxation, or unintentional non-taxation;
a) Efficiency: the costs of compliance to business and administration for governments should be minimized to the greatest extent possible;
a) Certainty and simplicity: tax rules should be clear and simple to enable taxpayers to understand them;
a) Effectiveness and fairness: taxation should produce the right amount of tax at the right time, and minimize the potential for evasion and avoidance;
a) Flexibility: taxation systems should be flexible and dynamic to ensure they keep pace with technological and commercial developments.

Proposed Measures are that Member States:

- To establish a National e-ID database and agency that are responsible for the issuance, storage and securing of online access of e-IDs and personal identities for verification and authentication, and for conducting e-KYC, which is accessible through approved API's;
- To develop a harmonized infrastructure for national biometrically authenticated e-ID service, which people can use to assert their identities in both face-to-face and remote identity transactions;
- To implement national e-ID and e-KYC frameworks for all persons and institutions that are integral to regional Real Time Payments (RTP);
- Citizens, MSMEs, companies, private institutions, Government/public entities (MDAs and NGOs in Member States have a unique ID numbers; There shall be a differentiation between the KYC documents required to on-board individuals and merchants etc. This will be done in accordance with the risk-based-approach in the banking sector.
- Develop cash-in-cash-out networks to provide backward compatibility with the legacy payment system - cash. This is implemented through an interoperable agent network across all payment streams;

- Develop a system of payments addressing: An interconnected payment system requires an addressing system whereby each potential payee is assigned a unique address. The use of more flexible addressing systems than the traditional bank/account number or phone number can offer payees additional convenience levels, which they can use to select their own addresses, and to payers who can deal with more memorable addresses. It can also help establish a competitive level playing field by ensuring that no single player gains control over the payment addressing system; and
- To facilitate inter-agency collaboration to ensure more coherent, efficient, and coordinated planning and implementation of proposed measures.
- Proposed electronic platforms and digital payment methods will have to comply with Member State's constitutions, national laws, national regulations, and their international obligations; especially national tax obligations and customs laws.

2.1.5 Data Privacy and Protection

Data and digital have become universal because of the: mobile revolution; spread of the internet following investments in infrastructure such as the undersea optical fibre cables; demographics (a significant part of population are aged below 34), who though living on low incomes, have embraced technology as the way of the future; and other ancillary factors, including pro-digital policy. Data has become central, not just in traditional financial services (e.g. credit information), but also in its application in the DFS, health, education, transport, and other aspects of daily life. Yet with these changes, the COMESA region still lacks a comprehensive policy and legal framework dealing with the key features of the "data economy", from its extraction from users, security, privacy, and protection of privacy. This might not be entirely unique to the region.

Most countries are considering their ability to manage "big data", because this is a cross cutting issue by nature, which has elements of national security as well, and therefore lacks a single institutional owner. Additionally, it is fast paced, and given the fact that technologies are constantly changing, policies can quickly become out-dated. Overall, having an over-arching policy, without attempting to address operational elements, would need to make provisions for crucial issues such as data mining, holding, protection and sharing. This leaves industry-specific standards and solutions that must be developed within these broad principles. In the financial sector, a foundational issue that a policy would help with is a situation in which the underlying philosophy is one of the supremacy of individual rights over their own data (bias toward individual rights), or whether the bias is toward use of data to inform product design (utilitarian approach). This would set the backdrop for all subsequent issues in terms of the mining, management, and sharing of customer's or individual's data.

Building an open digital payments system depends on the permitting of information flow without endangering the rights of individuals and businesses to privacy, and to determine the usage and disclosure of their data.

Proposed Measures are for Member States to:

- Develop domestic and cross-border regulatory cooperation to strengthen AML/CFT measures through data sharing and enforcement;
- Develop data protection, security and privacy provisions that facilitate the efficient flow of remittance transactions;
- Develop individual frameworks for financial data protection that encompasses the access, storage, and sharing of financial and non-financial data; and
- Harmonize individual frameworks into a single regional data protection framework.

2.1.6 Risk Management

The basic risks in the scheme are systemic, credit, liquidity, operational, legal, settlement, and information security risks. The Policy Framework defines these risks as follows:

- Credit risk: This refers to the risk that a counterparty, whether a participant or other entity, is unable to meet its financial obligations when they fall due, or either before or after the due date;
- Liquidity risk: This is the risk that a party in a payment flow, whether a participant or other entity, is unable to meet its financial obligations when due, although it may be able to do so in future. Liquidity risk might manifest in one or more of the scheme currencies;
- Compliance, legal and regulatory risks: These risks arise from an unexpected or uncertain application of a laws or regulations. These risks also crop up between financial institutions as they clear, settle, and effect payments and other financial transactions, and institutions must individually and collectively manage them;
- Settlement risk: This term is used to describe the risk that settlement in a fund will not take place as expected. This risk comprises of both credit and liquidity risk;
- Operational risk: This relates to inadequacies in internal processes, human errors, management failures, information technology systems or disruptions from external events that result in the reduction, deterioration, or breakdown of services provided by the scheme. The operational risk may include the following;
  - Operational risks on low-value, high volume RTP payments;
  - Resilience, reliability and security of core financial and payments infrastructure; and
  - Operational capacity and scalability of RTPs.

- Information security risk: This is the risk of loss resulting from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction of information assets and information systems.

The digital retail payments system is likely to be exposed to systemic risks and outages including:

- Online digital (hacking) risks;
- Denial of Service (DOS) and Man-in-Middle attacks;
- Failure of systemic Financial Market Infrastructures (FMIs) leading to payments systemic outage; and
- Communication Network failure between Digital Financial Service providers.

Specific risks related to data and privacy include:

- Customer data management and protection, including prior consent for use of personal customer data, meeting privacy of customer data under the GDPR-style, e-consumer protection laws, and standards for sharing customer data under open banking;
- Guarantees on data integrity and customer/ transaction data traceability; and
- Data privacy and confidentiality.

In order to mitigate against the effects and impact of these occurrences, the policy proposes that a Disaster Recovery Plan (DRP) be developed in case these risks occur. The plan would forestall any contamination from spreading to other interconnected systems and PSPs, thereby limiting the potential damages. This plan would also mitigate against the risk of interconnections with other systems, which are outside the payments system and networks, for example, e-ID databases.

Proposed Measures are that Member States should:

- Develop a DRP in the event of systemic risks and outages occurring; and
- Ensure that Mobile Money Operators (MMO) have put into place risk mitigation techniques to minimize operational, liquidity, technical, fraud, financial and money laundering risks.

2.1.7 Harmonization of Policies/Legislation

Implementation of a majority of the measures cited above will be done at the national level, followed by a harmonization process to be pursued regionally.

During consultations held with different stakeholders, including financial sector regulators, all were in agreement on the eight core policy areas that need harmonization in pursuit of regional COMESA payments framework, as follows:

- Anti-Money Laundering and the Combating of Financing of Terrorism Act (AML/CFT);
- Electronic Transactions Act (i.e., e-KYC, e- IDs, Electronic signatures etc);

- Interoperability across many technologies, platforms and systems in payments;
- Cyber security Act to protect digital payments platforms from cyber-attacks;
- Consumer protection guidelines for DFS;
- Banks and non-banks settlement system operating rules;
- National financial inclusion frameworks that include aspects of micro-finance policy; and
- Mobile money guidelines.

Besides the foregoing harmonization process in the eight policy areas, the stakeholders further agreed on the following four policy areas with regard to ICT infrastructure across the markets:

- Infrastructure Sharing Policy;
- Administrative Incentive Spectrum Pricing Policy;
- Quality of Service Guidelines; and
- Universal ICT Access Policy.

During the consultations, the financial sector regulators were particularly keen on the harmonization of cross-border retail payment policies. This would ensure affordable, transparent, and secure digital real time cross-border payments for MSMEs that can help increase intra-regional COMESA trade.

The business case report noted that a majority of the Member States have all these policies/legislations, although variations exist across the countries. This, therefore, calls for the harmonization option.

Proposed Measures are that Member States should:

- Comprehensively review the policy, legal and regulatory frameworks governing the payment system to determine their status in the region. The frameworks should also be examined to establish their suitability. These frameworks will facilitate implementation of the digital payment platform to be considered for harmonization; and
- Consider developing the eight proposed policies/ legislations, and four ICT policies in order to facilitate harmonization process at regional level if they do not have them.

2.2 Infrastructure for Payment Platform

2.2.1 Promoting Interoperability

Payment markets have become relatively diverse. Access to the payments infrastructure (including settlement facilities) has moved from traditional players, notably banks, to relatively new players, especially non-banks including mobile money operators and FinTechs.

Member States should continue supporting the introduction of interoperable systems both within and across the Member States. The systems, aimed at combining the mobile-enabled retail payments spaces into one, should be between all payment account issuers - both banks and non-banks. This would facilitate interoperable digital payments, an essential requirement if digital money is to be a competitive alternative to cash.

This can be achieved by developing common standards, and the Switch for common payments across Member States. Interoperability ought to create greater efficiencies, and result in the reduction of retail prices, while driving enthusiasm for service differentiation and innovation.

Proposed Measures

- One or more settlement entity shall be designated to work with both banks and non-banks as a net settlement agency;
- There is need for compliance with international standards and best practices for important payment platforms, including the Bank for International Settlements (BIS) standards for payment, Financial Management Information Systems (FMIS), and ISO 20022 (Standard for electronic data interchange between financial institutions);
- Conversion of the retail payments system to make it compliant with the Mastercard, and Visa (EMV), among other international card schemes, is necessary;
- The retail system to comply with the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system; and
- Development of common standards, and aspiring to develop a common payments' Switch across Member States.

2.2.2 Infrastructure Sharing Arrangement

2.2.2.1 Interconnecting Domestic Payment Infrastructure

A selected number COMESA Member States have a relatively well-developed mobile payment infrastructure, which other countries in the region can replicate. This will require interoperability among the Member States to facilitate interconnectivity of payment infrastructures as a solution to regional payments.

2.2.2.2 Expand Proprietary Closed-loop Bank Payment Systems/Networks

The other MSME payment solutions the region should consider are those that link end users of cross-border payments through commercial banks with the regional branch networks. For instance, KCB could offer seamless cross-border payments to

MSMEs across its regional bank and branch networks, including as a designated Net Settlement Entity

2.2.3 Standards in Payments

Standards are critical in the payment systems. They promote interoperability, permit data sharing, improve the functioning of the payment systems, sets out principles and guidance, and stipulate specifications for the services/products. The standards in payments address issues dealing with security of financial transactions, and either promote, facilitate or enable interoperability. The world is currently moving towards one common global standard for financial messaging, called ISO 20022. The global adoption of this standard is hastening, with a number of high-value payment market infrastructures, such as the Single European Payments Area (SEPA). This gives industry an opportunity to address friction points through the global adoption and implementation of ISO 20022, as the data standard for the cross-border payment ecosystem. Migration to ISO 20022 is crucial to overcoming challenges faced by the industry. It allows businesses, financial institutions, and other parties involved in financial transactions to exchange, interpret, and process payment information automatically. All countries globally are expected to adopt this standard by November 2022.

COMESA Member States should move alongside the rest of the world by exploring ways of adopting and implementing ISO 20022 to promote interoperability of payment systems in the region.

Proposed Measures

COMESA member states should explore ways of adopting and implementing ISO 20022 to promote interoperability of the payment system, including the adoption of other international standards in payment from organizations such as the: Financial Action Task Force (FATF); Committee on Payments and Market Infrastructures (CPMI); Society for Worldwide Interbank Financial Telecommunication (SWIFT); International Organization for Standardization (ISO); Payment Card Industry Data Security Standard (PCI DSS); and Mastercard and Visa Consortium (EMVCO).

Other Proposed Measures under Infrastructure are for Member States to:

- Develop, expand and grow an interconnected digital infrastructure in-line with the requirements of the dynamic ICT industry requirements of individual Member States and the region, as a whole;
- Promote digitization of government services across the country at affordable prices for those at the bottom of the financial pyramid;
- Support the development of a national strategy for payments towards the creation of a regional payment's utility. This should be complemented by the development of a regional payments infrastructure blueprint to inform the envisioned architecture;

- Facilitate the integration of clearing infrastructure to generate efficiencies, and support offers of near real-time payment across all major payment streams, encompassing structure and ownership of clearing houses, governance of the payment schemes, participation criteria, and the technical structure of the clearing network.
- Develop, and where necessary review and adopt common standards to support real-time transfers to make it easier to use various payment instruments encompassing standards, principles and procedures on payments such as QR code payments, NFC payments, mobile push payments, domestic card payments and card-less withdrawals.
- To facilitate the emergence of effective interchange fees where it is required to enable or promote interoperability between banks and non-banks.
- Promote cross-border payment solutions starting with a comprehensive diagnostic to identify constraints and solutions for regional and global payments, including examination of both payments regionally and private cross-border payment platforms.

2.3 Incentives for Use and Access

2.3.1 Mobile Money Guidelines

Competition among providers and networks will be a major factor for reducing transaction costs. Mobile money has revealed that the applications of a low-value payments solution can allow value to be transferred readily across space. This has driven revolution in the retail market in countries across the world. Mobile money is driving the uptake of DFS and cross-border real-time payments.

The transaction fees on the digital payments platform is expected to be equivalent to or less than domestic charges on similar payment transactions. In exceptional cases, the charges and fees for complex transactions should not exceed 0.75% of the payment value.

Proposed Measures are for Member States to:

- Explore ways in which various payment instruments can be easily accessible to disadvantaged groups;
- Encourage competition among providers and networks with the aim of reducing transaction costs;
- Put into place incentives for low cost transactions through an equivalent of domestic charges, and in exceptional cases, for complex transactions charges and fees not exceeding 0.75% of the payment value;
- Develop an Administrative Incentive Spectrum Policy, which considers aspects, such as geographical location and capacity of frequencies, among others. This will encourage Mobile Network Operators to install and commission network services in rural areas;

- Consider reviewing requirements and restrictions on who should operate and serve as an agent, including security requirements. A few limitations on agents may allow greater access of services by the unbanked;
- Promote the development and implementation of a broadband policy to assist Member States to leverage the full benefits of high speed and high quality connectivity;
- Explore financial incentives in order to promote mobile money uptake;
- Address the pricing of different aspects of digital payment related to taxation, because it is a critical component of determining access and usage of the DFSs;
- Propose measures for the reduction of the cost of devices, especially end user devices such as smartphones, etc. There is need to work with suppliers in the region to ensure that devices are affordable, especially for those at the bottom of the financial pyramid; and
- Develop tailor-made solutions, including bundles for MSMEs to facilitate access to DFSs.

2.3.2 Digital Financial Inclusion

It is important to expand the definition of financial inclusion beyond the mere holding of a bank account. Bank account ownership for the population aged over 15 years either at a regulated financial institution or with a mobile-money-service provider is considered a major metric associated with, and mostly used to describe "financial inclusion".

The MSMEs within the COMESA Region, including those that engage in cross-border retail trade, encounter challenging national and regional barriers to DFI. These include obstacles to the adoption by consumers of digital payments, gaps in the policy framework, and physical infrastructure at national and regional levels, which need be addressed.

Partnerships between DFSPs popularly called FinTechs and traditional commercial banks and intermediaries (PSPs) have the potential of meeting some of the financial and payment needs of MSMEs. The banking and financial sector regulators among the COMESA Member States have a role to play in expanding FinTech-enabled DFI.

Thus, DFI requires Member States to enable MSMEs to leverage on their information capital (in place of physical collateral). This will enable them access higher value-added DFSs with the proper safeguards in place for data protection and privacy.

Increasing MSMEs' access to DFSs and cross border retail payments is one of the public policy objectives of COMESA Member States. While the starting point is an account - whether a traditional bank account or a mobile wallet - the end goal is putting into place DFSs that address the needs of MSMEs and customers. These DFSs include digital versions of savings, payments, lending, and risk management products that help MSMEs mitigate against risks, reduce losses during unexpected events, and invest in their businesses at opportune moments (e.g. stocking up on seasonal commodities when prices are favorable).

The digital information collateral of MSMEs can flow from their digital financial transactions and payments footprint. The PSPs and DFSPs can use the financial and credit history of MSMEs resulting from regular or variable purchasing, selling, and cash flow patterns and informal digital credit arrangements to prevent contradiction within the Policy.

Proposed Measures are for Member States to:

- Develop clear and harmonized policy frameworks for enhancing access to DFSs and provide the strategic framework to guide these plans. The policy framework could cover areas such as: enabling open digital financial infrastructure; enhancing innovation; systemic security and resilience; protecting consumers; ensuring fair and open competition; and nurturing future market development.
- Promote the use of agent banking by either authorizing or licensing Payment Service Providers.
- Engage with stakeholders about guidelines on the fees to be charged, and discuss limits to be placed on the same.
- Provide persons with disabilities with a suitable digital solution to enable them participate and benefit from the DFSs.
- Put into place measures to empower women and youth to enable them benefit from the digital payment initiative for MSMEs in the region.

2.4 Capacity Building for Stakeholders

The Business Case Report recommended that COMESA Member States should establish national programs to strengthen the capacity of MSMEs to increase their uptake of DFSs and solutions in national and regional markets. This would be done with the goal of boosting regional and intra-Africa trade. According to the report, the development of ICT technical skills and financial literacy of MSMEs are important industry drivers in Africa.

The first phase (The Business Case Study) and second phase (The Business Model) of the project, identified capacity strengthening of MSMEs as a crucial area that needed urgent action, in order to build a strong demand for the Digital Retail

Payment platform. In this regard, the technical skills capacity Building Program, which will primarily focus on digital trade for MSMEs, targeting at least 250 MSMEs drawn from five COMESA Member States has been planned. The MSMEs will receive digital literacy training on cross border trade, which is aimed will ensure that they understand the implementation and usage of the digital retail payments platform.
Similarly, the third Phase of the project will focus on developing the technical capacity of 10,000 MSMEs within two years, and stakeholders of digital payments platforms in the region. The capacity building sessions will emphasize on creating awareness on and marketing the platform to stakeholders, and capacity development.

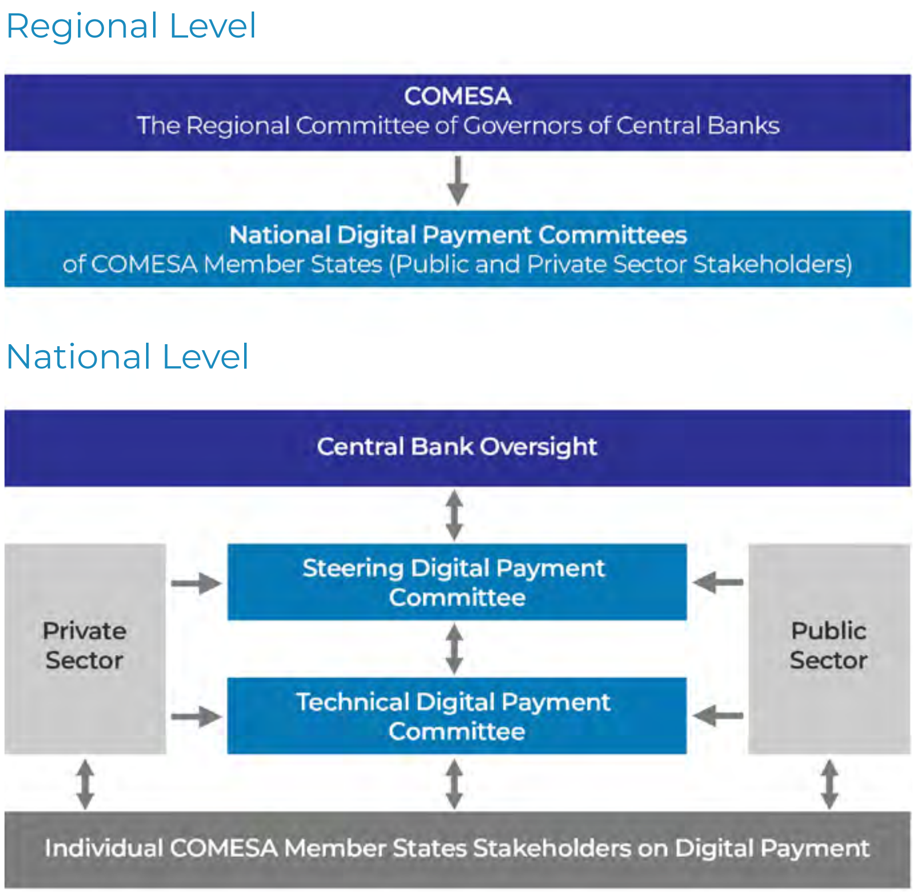
Proposed Measures for Member States are to:

- Train MSMES on access to, and utilization of digital payments platforms towards ensuring that they become users of the platform by the end of two years;
- Develop and nurture digital skills, values and culture among citizens of all Member States. This can be in the form of developing a training curriculum at all levels, mainstreaming of ICT in education curriculum, and integrating of soft skills into the digital training and workplaces, among others;
- Review the future capacity needs of regulators and policymakers, particularly with regard to the increasing use of innovative supervisory technologies;
- Implement a region-wide training program for MSMEs and stakeholders of the payments ecosystem; and
- Include the other key stakeholders in the region, such as the Chambers of Commerce in the capacity building program for MSMEs on digital financial literacy.

3 Institutional Arrangement

The successful implementation of this policy framework will depend on an effective, coordinated and functioning institutional arrangement, which has a strong political will and stakeholders' commitment.

Figure 2: Institutional Framework for implementation of the Policy on Digital Payment



The successful implementation of this policy framework will depend on an effective, coordinated and functioning institutional arrangement, which has a strong political will and stakeholders' commitment. This section sets out the institutional arrangements that will help implement the policy framework, and stipulates factors that must be take into consideration to facilitate the development and implementation of the digital payment platform.

The implementation arrangement provides for both top-down and bottom-up approach to issues that would arise during the implementation of the policy. In addition, the policy gives both the public and private sectors the opportunity to participate.

The Institutional arrangement will be implemented at both the regional and national levels. At the regional level, it is proposed that the Committee of Governors of the Central Banks will provide oversight on the implementation of the policy.

At the national level, while oversight of the policy will be done by the Central Banks, both the Steering and Technical Committees will manage its implementation.

The Steering Committee

Oversight will be provided by a Steering Committee comprising the Central Bank Governors of the Member States and drawing participation from multi stakeholder representation, with equal participation of commercial banks, mobile network operators, non-bank operators, ICT regulators and representatives of industry. The Committee will provide oversight to the implementation of the policy.

Table 1: Terms of Reference, Function and Composition of the Steering Committee

Role	Oversight	Composition
• Oversight of strategic alignment of the policy • Quarterly review of progress against plan • Management team challenge function • Approval of significant budget realignments • Approval of budget extension	• Approval of major new policy initiatives	• Central Bank governors • Payment regulators • Banks and Non-Banks

The Technical Committee

A technical committee with specific skills and expertise in the relevant areas will give technical oversight to the payment scheme. The committee, which will drive implementation of the key technical components, shall have linkages to the steering committee. Before the steering committee's meeting, the technical committee will be providing a brief quarterly report and develop a standard project monitoring sheet on a quarterly basis.

Table 2: Terms of Reference, Function and Composition of the Technical Committee

Role	Technical	Composition
• Management of primary relationships • Development and maintenance of work plan • Monitoring, updating of results framework • Monitoring performance against budget • Quarterly reports to project board • Summary reports for the PIC • Develop and manage procurement plan	• Identification of opportunities • Technical analysis of opportunities • Development of intervention proposals • Management of intervention execution • Results chain tracking • Formation and support of task teams • Risk analysis and control • Updating intervention results framework • Quality assurance	• Country teams

The roles and responsibilities of the Country Teams involved in the policy implementation:

a) The Central Bank: The Central Bank will provide oversight and regulate the payment systems. It shall also issue licenses to banks and payment service providers, besides supporting the community in the the adoption of digital financing

a) Settlement Agent: This will be one of the Central Banks among the COMESA Member States, and will settle the transactions undertaken by the system users

a) Financial/ICT Regulators: The regulators will help regulate the financial/ICT aspects of the digital payment platform

a) Banks: The banks will facilitate the movement of funds between users

a) Non-Bank Operators (MNOs and FinTechs): These are non-bank institutions support that will support transactions on the digital payment platform

a) CBC Digital Financial Services Association: This refers to a Special Purpose Vehicle (SPV), which will help in the development and implementation of the digital payment platform. In addition, the SPV shall be responsible for monitoring the transactions and AML/CFT activities.

In order to accomplish the desired change, implementation will depend on working with the key stakeholders identified in the preceding section. While regulators and policymakers will take a leading role in changing the rules and policy frameworks, the regulators will be in charge of directly implementing some of the policy proposals. As the payment's regulators, the Member States' Central Banks or payment regulators shall be the ultimate enforcers of compliance with regulations. Thus, increasing their capacity will help in ensuring long-term effectiveness in providing direction and oversight in the regional payments market.

4 Monitoring & Evaluation

Activities for each policy area have been defined and a clear results chain outlined to show how each activity will deliver an outcome.

Monitoring and evaluation are important tools in implementation and giving feedback to the policy framework and support programs towards meeting the set objective. This helps the policy makers respond to any issues that may arise in a timely manner. The policy framework will be delivered through four key policy objectives, which will seek to impact on the regional retail payments market level. Activities for each policy area have been defined and a clear results chain outlined to show how each activity will deliver an outcome. The policy makers will continuously track key learning points and make the necessary adjustments when needed. Flexibility will be necessary in the addition or removal of activities based on results, and towards ensuring that the projects remain dynamic and relevant to the market. The technical committee will develop any arising changes to activities in the context of the overall policy strategy. In case the change is significant enough, the same will be referred to the steering committee, before further action is taken.

A policy framework requires continuous monitoring and evaluation in order to ensure that the defined objectives and actions are being performed and are producing the intended outcomes. The Regulators providing the oversight (Central Banks) in consultation with relevant stakeholders, shall define a plan with milestones and performance indicators, which can be presented to, and periodically updated for the National Steering Committee meetings.

4.1 Implementation Matrix

Following the necessary consultations and participation of various categories of stakeholders, and upon the approval of this model policy framework, its implementation shall proceed as detailed in the following section. The implementation plan presented in the table below highlights all the activities that will be carried out, the time frame, and the entities responsible or to be involved in the implementation of the policy action.

Table 3: Implementation Matrix

Policy Pillar 1: Legal and Regulatory Framework for Payment Platform

Policy Action	Policy Measures	Timeframe	Organizations Responsible/ Involved
Policy Area 1.1: Cyber Security	Member States to: • Develop national cyber security policy framework where non-existent. • Enhance the existing fraud and crime monitoring and detection frameworks by deploying an analytics-led approach • Develop tailored and continuous capacity building for security stakeholders to better understand crimes related to payments. • Develop a cyber -security capacity building program. • Have a structured way of incident reporting and knowledge/incident sharing. This will enable entities to learn from each other as peers and guard against common crimes and create common responses. • Address cyber security framework that addresses the need of digital payment.	12 months after approval of this policy framework	ICT Regulators
Policy Area 1.2: Consumer Protection	Member States to: • Establish data protection, security and privacy provisions that facilitate the efficient flow of remittance transactions. • Develop effective awareness programs to empower consumers.	12 months after the approval of the Policy framework	• Ministries of ICT Finance and Trade, • Central Banks,

Policy Area 1.2: Consumer Protection (continued)	• Develop and adopt a uniform COMESA digital financial consumer protection consistent with the EU's General Data Protection Regulation (GDPR) framework, a widely accepted global standard on consumer protection and data/ information privacy. • Support Payment Services Providers (PSPs) and payment intermediaries to implement regular and continuous programs of consumer and user financial education to increase digital financial literacy in consultation with financial sector regulators. • Establish disputes resolution mechanisms to allow simple, low-cost ways to provide accessible redress and to deal with large numbers of uncomplicated retail problems without involving the court system. • Cooperate through multi stakeholder participation in financial literacy/education programs. • Develop and enforce cross-industry standards for addressing and resolving customer complaints on a timely and efficient basis which are appropriate to the specific needs of customers and the delivery channel.		• National Payment Services Providers, National Clearing Houses and Switches, Private Sector Associations

Policy Area 1.3: Ant-Money Laundering/ Combating Financing of Terrorism	Member States to: • Consider enacting Anti-Money Laundering/CFT legislation in case they lack one • Strengthen national legislation dealing with illicit financial flows • Consider increasing provision of financial integrity information and creating awareness on financial integrity to relevant stakeholders.	12 months after approval of this policy framework	• Central Banks, • Ministry of Finance, • Financial Intelligence Centres.
Policy Area 1.4: Electronic Transactions	Member States should: • Establish a National Digital Identification Database and e-ID Database Agency responsible for issuance, storage and secure online access of digital National IDs and personal identifies for verification and authentication and for conducting e-KYC accessible through approved APPs. • Develop a harmonized infrastructure for national digital identity service, biometrically authenticated, that people can use to assert their identity in both face to face and remote identity transactions. • Implement national digital Identification and e-KYC frameworks for all persons and institutions that are integral to regional RTP.	24 months after the approval of this policy framework	• Ministry of ICT. • Ministry of Finance, • ICT

Policy Area 1.4: Electronic Transactions (continued)	• Develop Cash-in-Cash out networks to provide backward compatibility with the legacy payment system – cash. This is generally implemented through an interoperable agent networks across all payment streams. • All citizens, MSMEs, companies, private institutions; Government/ public entities (MDAs and NGOs in Member States to have a unique ID number. • Facilitate Inter-agency collaboration to ensure more coherent, efficient and coordinated planning and implementation of proposed measures. • Develop a system of payments addressing: An interconnected payment system requires an addressing system whereby each potential payee is assigned a unique address. The use of more flexible addressing systems than the traditional bank/account number or phone number can offer added level of convenience to payees who can select their own addresses, and to payers who can deal with more memorable addresses. It can also help level the competitive playing field by ensuring that no single player gains control over the payment addressing system.		• Regulators, • Central Banks, • Private Sector Associations

Policy Area 1.5: Data Privacy and Protection	Member states should: • Develop domestic and Cross-border Regulatory Cooperation to strengthen AML/CFT measures through data sharing and enforcement • Develop data protection, security and privacy provisions that facilitate the efficient flow of remittance transactions. • Development of Disaster Recovery Plan (DRP) in the event of occurrences of systemic risks and outages. • Develop individual frameworks for financial data protection that encompasses the access, storage and sharing of financial and non-financial data. Individual frameworks across the Member States to be harmonised into a single regional data protection framework. • The MMO must ensure that risk mitigation techniques are in place to minimize operational, liquidity, technical, fraud, financial and money laundering risks.	6 Months after approval of this policy framework	• Central Banks, • ICT • Regulators, Bank and Non-bank Operators

Policy Area 1.7: Harmonization of Policies/Legislation	• Conduct a comprehensive review of the Policy, legal and regulatory framework governing payments system to identify determine the status of legal and regulatory framework in the Member States and examine the suitability of existing Policy, legal and regulatory framework that govern payment systems in the Member States that can facilitate implementation of digital payment platform to be considered for harmonisation. • Countries without any of these eight policies/ legislations and four ICT policies to consider develop them in order to facilitate harmonization process at regional level.	15 months after approval of this policy framework	• Ministries of ICT and Finance, • Central Banks, ICT Regulators, Bank and Non-bank Operators, • National Revenue Authorities, Private Sector

Policy Pillar 2: Infrastructure for Payment Platform

Policy Action	Policy Measures	Timeframe	Organizations Responsible/ Involved
Policy Area 2.1: Promoting Interoperability	• One or more central bank(s) shall be designated as a net settlement entity. • There is need for compliance with international standards and best practices for systemically important payment platforms including Bank for International Settlements (BIS) standards for payment and Financial Management Information Systems (FMIS) • The retail payment system to be Europay, Mastercard, and Visa (EMV) compliant. • The retail system to comply with the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system. • Development of common standards but also aspiring to develop a common payments switch across Member States.	12 months after approval of this policy framework	• Central Banks

Policy Area 2.2: Infrastructure Sharing Arrangement	Member States to: • Undertake an assessment of the current payments infrastructure and define opportunities for investments in infrastructure that will broaden access and produce cost efficiencies. • Share views and experiences with each other and with the private sector on FinTech developments and country responses using international fora as conduits. • Develop and enforce infrastructure sharing guidelines in critical infrastructure such as towers, ATM machines, data centers, etc, so that the cost of Network Operational Expenditure (OPEX) is low. As long as it is technically and economically feasible, network elements are expected to be shared. • Develop Universal ICT Access policies so that there is seamless geographical network coverage • Comply with Key Performance Indicators (KPIs) set up by regional and International bodies like Bank for International Settlements (BIS), International Telecommunications Union (ITU), etc	6 months after approval of this policy framework	• Central Banks, ICT Regulators, Bank and Non-bank operators

Policy Area 2.2: Infrastructure Sharing Arrangement (continued)	• Foster an enabling digital innovation ecosystem that can navigate technological revolutions and establishment of a sustainable conducive environment for the utilization of emerging technologies through introduction of regulatory sandboxes which lead to more FinTech start-ups • Besides adopting collaborative regulatory approach between in-country ICT and Financial sector regulatory authorities, considerations should be made to formulate cross-border regulatory collaborations through MOUs for the converging industries.		
Policy Area 2.3: Other Policy Areas Under Infrastructure	Member States to: • Develop, expand and grow an interconnected digital infrastructure in line with the dynamic ICT industry requirements of individual Member States and the region as a whole. • Promote digitization of government services across the country. • Support the development of a national payments' strategy towards creation of a regional payments' utility. This should be complemented by the development of a regional payments infrastructure blueprint to inform the envisioned architecture.		

Policy Area 2.3: Other Policy Areas Under Infrastructure (continued)	• • Facilitate the integration of clearing infrastructure to generate efficiencies and support near real-time payment offerings across all major payment streams, encompassing structure and ownership of clearing houses, governance of the payment schemes, participation criteria and the technical structure of the clearing network. • Develop, and where necessary review and adopt, common standards to support real-time transfers to make it easier to use various payment instruments encompassing standards, principles and procedures on payments such as QR code payments, NFC payments, mobile push payments, domestic card payments and card-less withdrawals. • Facilitate the emergence of effective interchange fees where it is required to enable or promote interoperability. • Promote cross-border payments solutions starting with a comprehensive diagnostic to identify constraints and solutions for regional and global payments including examination of both regional payment and private cross-border payment platforms.		

Policy Pillar 3: Incentives for Use and Access

Policy Action	Policy Measures	Timeframe	Organizations Responsible/ Involved
Policy Area 3.1: Mobile Money Guidelines	Member States to: • Explore ways in which various payment instruments can be easily accessed by disadvantaged groups. • Encourage competition among providers and networks bring down transaction costs. • Put in place incentives for low-cost transaction through an equivalent of domestic charges and in exceptional cases for complex transactions charges and fees not exceeding 0.75% of the payment value. • Develop Administrative Incentive Spectrum Policy which looks at aspects such as geographical location, bandwidth of frequencies and others. This will encourage Mobile Network Operators to install and commission network services in rural areas. • Consider reviewing requirements and restrictions on who should operate and serve as an agent, including security requirements. If there are few limitations on agents, it may allow greater access of services by the unbanked.	6 months after approval of this policy framework	• Ministries of Finance, Central Banks, • ICT Regulators, Customs and revenue Authorities, Banks and Non-bank operators

Policy Area 3.1: Mobile Money Guidelines (continued)	• Promote the development and implementation of broadband Policy to assist Member States to leverage the full benefits of high-speed and high – quality connectivity. • Explore tax incentives in order to promote mobile money uptake • Address the pricing of digital payment aspects related to taxation because it is a critical component in determining access and usage of the DFSs. • Propose measures for the reduction of the cost of devices especially end user devices like Smartphones etc. There is a need to work with Suppliers in the region to ensure that devices are affordable especially for the bottom of the financial pyramid. • Develop tailored made solutions like bundles for MSMEs to facilitate access to DFSs.	6 months after approval of this policy framework	• Ministries of Finance, Central Banks, • ICT Regulators, Customs and revenue Authorities, Banks and Non-bank operators

Policy Area 3.2: Digital Financial Inclusion	Member States to: • Develop clear and harmonized policy frameworks for enhancing access to DFSs and provides the strategic framework to guide these plans. The policy framework could cover areas such as: enabling open digital financial infrastructure; enhancing innovation, systemic security and resilience; protecting consumers; ensuring fair and open competition and nurturing future market development. • Promote the use of agent banking by authorizing or licensing Payment Service Providers. • Engage with stakeholders concerning guidelines on the fees to be charged and discuss limits to be placed on such fees. • Provide persons with disabilities with the platform to participate and also benefit from the DFSs • Put measures to empower women and youth to benefit from digital payment initiative for MSMEs in COMESA region.	12 months after approval of this policy framework	• Ministry of ICT, • Ministry of Finance, Ministry of Trade (MSMEs), • Central Banks, • ICT Regulators

Policy Pillar 4: Capacity Building for the Stakeholders

Policy Action	Policy Measures	Timeframe	Organizations Responsible/ Involved
Policy Area 4.1: Capacity Building	• MSMEs to be trained to access and usage of digital payments platforms of the operation of the digital payments platforms and have become users of the COMESA digital retail payments platform at the end of two years. • Develop and nurture digital skills, values and culture across the citizenry of all Member States. This can be in the form of training curriculum at all levels, mainstreaming of ICT in education curriculum, integration of soft skills into the digital skills training and workplaces, etc. • Review of the future capacity needs of regulators and policymakers, in particular around the increasing use of innovative supervisory technologies. • Implement a region-wide training program for MSMEs and stakeholders of the Payments ecosystem. • The other key stakeholders in the COMESA can be included in the capacity building program for MSMEs on digital financial literacy such as Chambers of Commerce.	24 months after approval of this policy framework	• Private Sector, Industry-MSMEs and Women in Trade, Payments stakeholders. • Chambers of Commerce.

Institutional Arrangement for Implementation of the Policy

National Steering Committees	• Member States to constitute National Steering Committees	2 months after approval of this policy framework	• National Central Banks • In consultation with Ministries of Finance and ICT
National Technical Committees	• Member States to constitute National Technical Committees	2 months after approval of this policy framework	• National Financial/ ICT Regulators in consultation with Central Banks, • Ministries of Finance and ICT
Digital Financial Services Association	• Establishment of Digital Financial Services Association	6-12 months after approval of this policy framework	• COMESA Business Council, Private Sector Institutions in consultation with Financial Regulators.

COMESA Business Council
COMESA Building, Right Wing, 2nd Floor
Ben Bella Road, P.O. Box 30051, Lusaka, Zambia
comesabusinesscouncil.org