

# Navigating Mobile Money Regulatory Risks





---

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive.

Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at [www.gsma.com](http://www.gsma.com)

Follow the GSMA on X: [@GSMA](https://twitter.com/GSMA)

---

## GSMA Mobile Money

The GSMA's Mobile Money programme works to accelerate the development of the mobile money ecosystem for the underserved.

For more information, please contact us:

[www.gsma.com/mobilemoney](http://www.gsma.com/mobilemoney)

X: [@GSMAMobileMoney](https://twitter.com/GSMAMobileMoney)

[mobilemoney@gsma.com](mailto:mobilemoney@gsma.com)

### Authors

**Kennedy Kipkemboi Sawe**, Public Policy & Advocacy Director,  
Mobile Money, GSMA

**Tarunpreet Singh**, Regulatory Specialist, Mobile Money, GSMA

### Contributors

**Ashley Olson Onyango**, Head of Financial Inclusion & AgriTech, GSMA

**Tony K. Ngige**, Stealth Africa Consulting LLP

© 2024 - GSMA



# Contents

---

	Executive summary	05
<b>01</b>	Introduction	09
	1.1 Evolution of mobile money risks	11
	1.2 Risk management frameworks	12
	1.3 Risk management typology and classification	13
<b>02</b>	Survey insights: key regulatory risks	15
	2.1 Cybersecurity and fraud risks	17
	2.2 AML/CFT risks	18
	2.3 Licensing and registration complexities	18
	2.4 Data protection and privacy risks	19
<b>03</b>	Barriers to effective regulatory risk management	20
	3.1 Overregulation and uncertainty: the industry's double burden	22
	3.2 Compliance challenges: a costly endeavour	24
<b>04</b>	Case studies: navigating regulatory risks	25
	4.1 Strengthening Sri Lanka's AML/CFT framework and the need for higher transaction limits	26
	4.2 Strides in Ghana to boost digital finance despite challenges	27
	4.3 Challenges and progress in Pakistan's financial inclusion and regulatory landscape	28
	4.4 Kenya's digital finance framework	30
	4.5 Nigeria's regulatory framework and the impact on risks	31
	4.6 Mandatory biometric SIM card registration in Tanzania for KYC	31
	4.7 Other regulatory risk mitigation initiatives	32
<b>05</b>	Structured approach to regulatory risk management	33
	5.1 Risk assessment tools	36
	5.2 Risk management tools	39
<b>06</b>	Conclusion	41
<b>07</b>	Recommendations	44

---

## Acronyms and abbreviations

<b>AI</b>	Artificial Intelligence	<b>ID</b>	Identity Document
<b>AML/CFT</b>	Anti-Money Laundering/Combatting the Financing of Terrorism	<b>KRI</b>	Key Risk Indicator
<b>BoG</b>	Bank of Ghana	<b>KYC</b>	Know Your Customer
<b>BoT</b>	Bank of Tanzania	<b>MMP</b>	Mobile Money Provider
<b>CBK</b>	Central Bank of Kenya	<b>MNO</b>	Mobile Network Operator
<b>CBN</b>	Central Bank of Nigeria	<b>MTN</b>	Mobile Telephone Network
<b>CDD</b>	Customer Due Diligence	<b>NADRA</b>	National Database and Registration Authority
<b>COSO</b>	Committee of Sponsoring Organisations of the Treadway Commission	<b>NPS</b>	National Payment System
<b>DFS</b>	Digital Financial Services	<b>OTC</b>	Over The Counter
<b>DPI</b>	Digital Public Infrastructure	<b>PII</b>	Personally Identifiable Information
<b>DPO</b>	Data Protection Officer	<b>PPP</b>	Public-Private Partnership
<b>DTS</b>	Digital Transfer Service	<b>PPI</b>	Prepaid Payment Instrument
<b>eKYC</b>	Electronic Know Your Customer	<b>PSB</b>	Payment Services Bank
<b>FATF</b>	Financial Action Task Force	<b>PSP</b>	Payment System Operator
<b>FIU</b>	Financial Intelligence Unit	<b>SIM</b>	Subscriber Identity Module
<b>GDPR</b>	General Data Protection Regulation	<b>SBP</b>	State Bank of Pakistan
<b>GhQR</b>	Ghana National Quick Response	<b>UPI</b>	Unified Payment Interface

## Figure List

Figure 1	Mobile money risk management typology and classifications	13
Figure 2	Key regulatory risks identified from the survey	16
Figure 3	Proactive risk mitigation measures employed by MMPs	19
Figure 4	Summary of challenges identified in the mobile money sector	21
Figure 5	How regulatory issues affect business	23
Figure 6	Risk management practices in place	34

## Table list

Table 1	The evolution of mobile money risks	11
Table 2	Examples of qualitative and quantitative risk measures	35
Table 3	Example of an impact measurement guide	37
Table 4	Example of a likelihood guide	38
Table 5	Risk score guide	38

# Executive summary



# Executive summary

---

Mobile money platforms are integral to expanding financial inclusion, but they face mounting regulatory risks due to evolving fraud, cybersecurity, AML/CFT and data privacy concerns.

The survey highlights that MMPs are most concerned about cybersecurity and fraud risks (68.97%) and anti-money laundering/combating the financing of terrorism (AML/CFT) risks (62.07%), followed by challenges related to licensing and registration complexities (55.17%) and data protection (44.83%). As demonstrated in this report, mobile money providers (MMPs) must adopt comprehensive risk management frameworks, such as ISO 31000 and COSO, to mitigate regulatory risks and ensure operational resilience. The integration of emerging risk categories, such as Environmental, Social and Governance (ESG) risks, highlights the need for a holistic approach to managing the interconnected nature of risks, particularly reputational harm. Case studies and typologies show that effective risk management strategies, combined with robust third-party oversight, are essential for MMPs to remain competitive and compliant in increasingly regulated environments. By adopting structured and forward-looking frameworks, MMPs can safeguard their services, build stakeholder trust and foster innovation within the rapidly digitising financial sector.

---

81.48% of the respondents believe that existing regulations are lagging technological advancements.

As technologies like blockchain, AI and mobile payments evolve, existing regulations often fail to address the unique risks they present, creating uncertainty for businesses that lack clear regulatory guidance.

---

75.86% of the respondents found regulations to be unbalanced and unsuitable, with 44.83% specifically viewing them as overregulated.

Overregulation has led to business closures in markets like Kenya, where stricter regulatory requirements forced smaller MMPs to exit due to escalating compliance costs. The regulatory changes often demand substantial investments in systems, staff training and compliance infrastructure, disproportionately burdening smaller MMPs. One survey respondent reported annual losses of up to USD 100,000, underscoring the significant financial strain regulatory compliance places on MMPs. This not only hampers operational efficiency but also restricts market agility, making it harder for smaller providers to remain competitive and innovate.



MMPs show robust compliance, with 72.41% aligned with regulations and 75.86% adopting formal strategies, though only 70.37% integrate risk appetite.

MMPs have demonstrated robust risk management practices, with unanimous adherence (100%) to independent board oversight, formal reporting mechanisms, dedicated risk management teams and business continuity and disaster recovery planning. High-priority measures, including formal risk assessments, technology-driven controls (e.g. 2FA), transaction monitoring systems and incident response plans, are implemented by 96.30% of respondents. Formal risk management policies and education programmes also receive significant attention at 92.59%, while tools such as key risk indicators (KRIs) and dashboard management logs are used by 81.48% of respondents. However, risk appetite and limits, while important, are integrated by only 70.37%, indicating a potential area for further strengthening risk frameworks.

Reputation becomes the ultimate risk, as MMPs navigate nine interconnected risks, now evolving to encompass ESG considerations.

In the increasingly complex landscape of mobile money, reputational risk emerges as the central and most significant consequence, acting as the cumulative result of poorly managed risks across nine critical areas: strategic, regulatory, operational, technology, fraud, third-party, financial, ESG and country. The interconnected nature of these risks amplifies their impact, where a failure in one area can trigger a cascade of adverse effects across others, ultimately jeopardising the provider's reputation. While traditional risks persist, contemporary concerns like ESG have emerged, pressing MMPs to assess environmental impacts such as digital waste and prioritise transparency, ethical practices and regulatory compliance on the governance front.

---

With  $\frac{3}{4}$  of MMPs struggling with manual processes and outdated tools, they must embrace AI-driven regtech, sandboxes and cloud solutions to overcome regulatory challenges.

MMPs are increasingly hindered by manual processes (77.78%) and outdated tools (66.67%), leading to errors, delays and poor decision-making, which can have detrimental impacts on compliance and overall efficiency. MMPs must innovate to remain competitive and compliant in an increasingly complex regulatory environment. Traditional rule-based risk management systems, such as fraud management and transaction monitoring, often fall short in detecting sophisticated threats, emphasising the need for advanced solutions. Regtech, with its AI-driven capabilities, offers real-time fraud detection, streamlined compliance and adaptability to evolving regulations, while regulatory sandboxes foster innovation under controlled conditions, ensuring compliance without stifling creativity. Additionally, cloud-based compliance tools enhance scalability and accessibility, enabling MMPs to reduce costs and meet regulatory demands effectively.

---

While regulatory frameworks for mobile money have progressed globally, there remain significant opportunities to alleviate growth constraints.

While Sri Lanka made significant progress in addressing strategic AML/CFT deficiencies, leading to its successful removal from the Financial Action Task Force (FATF) grey list in 2019, MMPs highlighted the financial strain of stringent AML/CFT protocols on mobile money operations, exacerbated by low transaction limits and bank-like compliance requirements. In Pakistan, while there have been notable advancements in financial inclusion through branchless banking, issues such as restrictive pricing limits and non-inflation linked transaction limits must be addressed to further support the sector. Kenya, a pioneer in mobile money innovation with M-PESA, faces challenges with a lack of government-driven identity verification solutions and regulatory setbacks, including its grey-listing by the FATF in 2024. Nigeria's mobile money regulatory framework offers strong consumer protection but has been criticised for stifling innovation. Tanzania's biometric SIM card registration initiative has significantly reduced fraud but faces ongoing challenges with data privacy concerns and the requirement for national ID registration.

Based on this research, the GSMA provides recommendations (see [Section 7](#)) emphasising the importance of clear, consistent and proportionate regulations tailored to risks. A risk-based approach by regulatory bodies, collaboration between regulators and industry for adaptable frameworks and leveraging technologies to manage risks effectively are key strategies. The use of structured risk assessment tools enables MMPs to evaluate risks comprehensively and prioritise their management based on financial, reputational, regulatory and legal impacts.



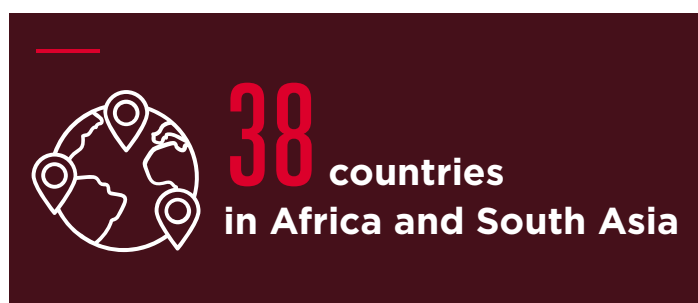
# 01 Introduction



Digital financial services (DFS), especially mobile money, have had a transformative impact on financial inclusion but face growing challenges from regulatory risks. These risks, driven by changing laws and regulations, can disrupt business operations, increase costs and affect strategy. They are further complicated by factors such as fraud and cybersecurity threats.

From 2008 to 2018, banks and other financial institutions were fined nearly USD 27 billion globally for failing to comply with anti-money laundering/combating the financing of terrorism (AML/CFT) and know-your-customer (KYC) regulations. Such compliance risk is difficult to assess with traditional approaches.<sup>1</sup> Effective risk management is key to safeguarding the future of mobile money platforms.

This report aims to provide an understanding of current knowledge, practices and trends in regulatory risk management for mobile money. It explores how mobile money providers (MMPs), particularly in Africa and South Asia, are adapting to changing regulatory environments while remaining competitive. The report is based on the findings of a regulatory risk survey and interviews with key stakeholders in the mobile money ecosystems of 38 countries. The report explores regulatory risks and challenges such as cybersecurity, AML/CFT and data protection, and presents case studies of how different countries have approached these challenges. The report also highlights important frameworks and tools available for MMPs to monitor and mitigate these challenges.



This report captures the views of stakeholders from across the mobile money ecosystem. 46.88% of survey respondents represent mobile network operators (MNOs), 28.13% are from the fintech sector, 12.50% from financial institutions and the rest, 12.49%, are DFS regulators, consultants, agents and third parties. 72% of respondents are experienced professionals who provide significant expertise in the mobile money sector and within their organisations.

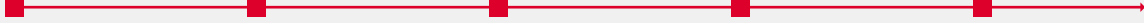
<sup>1</sup> Qureshi, M.W. (1 July 2019). "Understanding compliance risk in finance and banking". ISACA.

# 1.1 Evolution of mobile money risks

Table 1 shows the evolution of mobile money risks over key phases of development. Each phase is marked by advancements in service maturity and corresponding regulatory responses that shaped how risks were managed. It highlights the progression from foundational operational risks and regulatory challenges to more complex, technology-driven risk management frameworks, with a focus on resilience and harmonisation in the digital age. By understanding these shifts, stakeholders can better navigate current and future challenges to ensure safe, inclusive and innovative financial ecosystems.

Table 1

## The evolution of mobile money risks



	<b>2007 – 2010</b> <b>Early mobile money</b>	<b>2010 – 2013</b> <b>Establishing standards</b>	<b>2013 – 2015</b> <b>Risk frameworks</b>	<b>2015 – 2020</b> <b>Regulatory challenges</b>	<b>Beyond 2020</b> <b>Post-COVID considerations</b>
<b>Key developments</b>	Launch of basic mobile money services like M-Pesa in Kenya. Undefined regulatory environment	Specific regulations introduced for AML/CTF and KYC compliance  Cross-border transactions increase.	Implementation of structured risk assessment and FATF guidelines. Focus on market competition	<ul style="list-style-type: none"> <li>Global expansion of mobile money</li> <li>Cybersecurity emphasis</li> <li>Adoption of new tech like cryptocurrencies</li> </ul>	Digital transformation accelerated, focus on digital resilience and consumer protection
<b>Risk focus</b>	<ul style="list-style-type: none"> <li>Operational risks (fraud, outages, agent misconduct), regulatory uncertainty, lack of data privacy frameworks</li> </ul>	<ul style="list-style-type: none"> <li>Consumer protection</li> <li>fraud prevention</li> <li>regulatory harmonisation challenges</li> <li>compliance complexities.</li> </ul>	<ul style="list-style-type: none"> <li>Cybersecurity</li> <li>Market competition</li> <li>Stress testing</li> <li>Systemic risk management</li> </ul>	<ul style="list-style-type: none"> <li>Cybersecurity threats</li> <li>Data protection laws (e.g. GDPR)</li> <li>Taxation issues</li> <li>Regulatory fragmentation</li> </ul>	<ul style="list-style-type: none"> <li>Digital resilience</li> <li>Safeguarding consumer data</li> <li>ESG integration</li> <li>Regulatory harmonisation</li> <li>Cross-border collaboration</li> </ul>

# 1.2

## Risk management frameworks

Risk management frameworks provide structured approaches for organisations to identify, assess, mitigate and monitor risks that may impact their objectives and operations. These frameworks, such as ISO 31000 and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework, offer standardised methodologies for organisations to integrate risk management in their strategic and operational processes, enhancing their ability to manage uncertainty, improve resilience and contribute to more informed strategic and operational decisions.<sup>2</sup> By following steps such as risk identification, evaluation and treatment, organisations can develop comprehensive strategies to mitigate adverse impacts and capitalise on potential opportunities.<sup>3</sup> This structured approach not only provides clarity, but also ensures that risk management practices align with international standards such as ISO 31000. In 2016, the IFC World Bank Group and the MasterCard Foundation published the *Digital Financial Services and Risk Management Handbook*, which offers a systematic approach to risk management for mobile money and DFS providers.<sup>4</sup> The overall framework is similar to, and aligned with, ISO 31000 and the COSO Framework.



<sup>2</sup> Ibid., p. 8.

<sup>3</sup> FERMA, 2011.

<sup>4</sup> Qureshi, M.W. (1 July 2019). "Understanding compliance risk in finance and banking", p. 8, ISACA.

# 1.3 Risk management typology and classification

The 2024 GSMA report, *Mobile Money Fraud Typologies and Mitigation Strategies*, suggests that standardisation has many benefits, including consistency, clear communication, efficiency, benchmarking and metrics and adaptability.<sup>5</sup> The IFC World Bank Group and MasterCard Foundation's *Digital Financial Services and Risk Management Handbook* provides the following risk

categories: strategic, regulatory, operational, agent management, technology partnership, fraud and financial. While these risk categories are still relevant to mobile money, this report proposes the following mobile money risk classification typology, which has been updated to include emerging risks such as Environmental, Social and Governance (ESG) risks.

Figure 1

Mobile money risk management typology and classifications



<sup>5</sup> GSMA. (2024). *Mobile money fraud typologies and mitigation strategies*.

This typology covers the primary risks for mobile money, elevating contemporary ones like ESG as a primary risk. For example, financial inclusion, which is a social risk and key objective of mobile money, has not been formally assessed in mobile money risk frameworks. MMPs must now also consider ESG risks such as the impact of digital waste on the environment. Reputational risk, positioned at the centre of the diagram to highlight its critical role and connection to all other risks, is best classified as a consequential risk. All nine primary risks – strategic, regulatory, operational, technology, fraud, third-party, financial, ESG and country – trigger events that, if unmanaged, lead to reputational harm. This perspective underscores how reputational impact is cumulative and multifaceted, and is directly related to how well other risk areas are managed. Reputational impact is assigned a distinct score within a mobile money risk assessment, which contributes to the overall impact score.

Risk management for mobile money requires a specialised and multilayered approach, tailored to address the unique challenges and interconnections. For example, fraud by a mobile money agent can be caused by technological weaknesses, which can then trigger regulatory sanctions and cause reputational damage. This interconnectedness is important to bear in mind during any risk management process. Unlike traditional financial services, where technology and fraud risks are often considered subsets of operational risk, mobile money risks need to be categorised independently due to their significant impact on service integrity, operational resilience and customer trust. Other risks, such as agent network management and partnership risks, are included in the third-party risk category, with a proposal that MMPs build strong third-party oversight programmes.

A comprehensive mobile money risk framework that encompasses strategic, regulatory, third-party, ESG and reputational risks, enables MMPs to better anticipate cascading impacts, prioritise risk areas and protect against a range of vulnerabilities in rapidly digitalising and increasingly regulated environments.

Integrating ESG considerations and country-specific risks in mobile money risk frameworks marks a shift towards more responsible and sustainable practices in digital finance. This approach helps MMPs meet global standards for sustainability and supports digital governance and regulatory compliance. By adopting a structured and forward-looking risk management model, MMPs can foster stakeholder trust, enhance resilience and effectively navigate the complexities of digital transformation in the financial sector.<sup>6</sup>

---

<sup>6</sup> For definitions and more information, see “[Digital Financial Services Risk Categories and Classification](#)” on the Stealth Advisors website.

# 02

## Survey insights: key regulatory risks



Regulatory risk arises when regulatory environments evolve in ways that impose new constraints, introduce unexpected costs or affect how an organisation operates. **Figure 2** highlights the key regulatory risk categories identified in the survey, which are elaborated below.





# 2.1

## Cybersecurity and fraud risks

According to the survey, 68.97% of respondents consider cybersecurity and fraud the most significant risk for mobile money from a regulatory perspective. Cybersecurity and fraud prevention were identified as the highest priority, reflecting the critical risks MMPs face from cyberthreats and fraudulent activities. Studies show that cybersecurity remains a top concern for regulatory authorities, with some suggesting that improvements in regulatory technology (regtech) solutions may help to address this concern.<sup>7</sup>

The United Nations Conference on Trade and Development (UNCTAD) reports that 13% of countries worldwide lack cybercrime-related legislation. These countries include the Democratic Republic of Congo (DRC), Somalia, Central African Republic (CAR), Liberia, Guinea and Bolivia, all of which have mobile money deployments.<sup>8</sup> As the mobile money ecosystem becomes increasingly digital, the inability to protect against cyberattacks threatens the overall stability of financial platforms. Even in jurisdictions with legislative frameworks, there are increasing cases of hacking, phishing, SIM swap fraud and account takeovers.<sup>9</sup> Mobile money platforms such as M-PESA have had to significantly upgrade their systems to prevent phishing attacks, unauthorised access and other cyberthreats.<sup>10</sup>

The rise in cyberattacks presents an opportunity for MMPs to adopt advanced cybersecurity measures. Leveraging regtech solutions could enhance real-time fraud detection and prevention through artificial intelligence (AI)-driven systems.<sup>11</sup> Beyond individual efforts, public-private partnerships (PPPs) present an opportunity to establish comprehensive cybersecurity frameworks.

---

7 Financial Industry Regulatory Authority (FINRA). (September 2018). *Technology Based Innovation for Regulatory Compliance ("RegTech") in the Securities Industry*.

8 UNCTAD. (July 2023). "Cybercrime Legislation Worldwide".

9 GSMA. (2024). *Mobile money fraud typologies and mitigation strategies*.

10 Trinity Analytica. (28 February 2024). "M-PESA Under Attack: Securing Kenya's Mobile Money Lifeline in the Age of Phishing and SIM Swaps".

11 Accenture. (2021). *2021 Cyber Threat Intelligence Report: Threats Unmasked*.

## 2.2

# AML/CFT risks

Anti-money laundering (AML) and combating the financing of terrorism (CFT) risks emerged as another top priority for survey respondents, underscoring the global regulatory pressure to prevent financial systems from being exploited for illicit activities. Ensuring compliance with AML/CFT regulations is particularly challenging given the complex nature of mobile money. Unlike traditional banking, mobile money operates in a unique ecosystem that blends telecommunications infrastructure, financial services and technology, which introduces several layers of complexity. Additionally, MMPs should adhere to both local laws and regulations and international standards, such as those set by the FATF.

Providers noted that the need to comply with changing AML/CFT regulations has forced them to make substantial investments in system upgrades. These compliance costs have made it difficult for smaller players to remain competitive in the market. An example is PrivPay, a Kenyan fintech offering anonymous M-PESA transactions, which was shut down in 2023 after Safaricom cut their API access due to concerns over compliance with AML/CFT regulations. Safaricom cited the need for a Central Bank of Kenya payment service provider (PSP) licence, which PrivPay did not have.<sup>12</sup>

There is an opportunity for MMPs to explore automated compliance systems that monitor and flag suspicious activities in real time, to reduce the costs and human resources dedicated to compliance.<sup>13</sup>

## 2.3

# Licensing and registration complexities

Licensing and registration complexities were identified as significant regulatory risks by 55.17% of respondents. The survey also indicated that 44.83% of respondents feel that overregulation is creating direct barriers to business, with newer market entrants the most affected. For MMPs operating across multiple jurisdictions, varied and sometimes ambiguous licensing requirements pose barriers to market entry and expansion.

Licensing and market entry challenges are pronounced in regions where regulatory bodies have not established clear frameworks for mobile money operations. In some markets, the regulatory burden of obtaining and maintaining licences is considered one of the most significant barriers to growth, especially for smaller MMPs.

For instance, in Ghana, the Payment Systems and Services Act (2019)<sup>14</sup> introduced stringent requirements for MMPs, including increased financial reserves, which have led to consolidation in the industry as smaller players struggled to meet the new requirements.

These challenges present an opportunity for regulatory reform and advocacy. Industry bodies could engage with regulators to promote more transparent, scalable and tiered licensing frameworks accessible to smaller MMPs.<sup>15</sup>

<sup>12</sup> Abuya, K. (13 August 2024). "PrivPay shutdown after Safaricom cut API access over compliance violations". *Techcabal*.

<sup>13</sup> FATF. (2023). *International standards on combating money laundering and the financing of terrorism & proliferation (FATF Recommendations)*, Section 10.

<sup>14</sup> Bank of Ghana. (2019). *Ghana's Payment Systems and Services Act, 2019*.

<sup>15</sup> England J. (26 January 2023). "New Fintech regulations and the changing climate of 2023". *FinTech Magazine*.

## 2.4

# Data protection and privacy risks

As MMPs manage increasing volumes of sensitive personal and financial data, data protection and privacy have become critical priorities as noted by 44.83% of the survey respondents. While many countries have introduced data protection regulations, such as frameworks modeled after the EU's General Data Protection Regulation (GDPR),<sup>16,17,18</sup> enforcement is inconsistent, leaving gaps that could lead to penalties.

Compliance has driven up transaction costs, disproportionately affecting lower-income users. Technological investments, such as data encryption, are necessary but often delay service roll-outs and increase onboarding time, ultimately reducing user adoption. One interviewee noted that implementing new data privacy standards in Ghana led to a 15% increase in onboarding time, negatively affecting user adoption rates.

Compliance with data privacy regulations not only fulfils legal requirements, but can also serve as a competitive advantage by fostering consumer trust and loyalty. Prioritising data security signals to customers that their information is valued and protected, which can strengthen brand reputation. Investing in advanced encryption technologies, secure data management systems and seamless onboarding processes can enhance user experiences, reduce friction and build consumer confidence. At the same time, these efforts ensure adherence to regulatory standards, positioning MMPs as proactive and trustworthy market leaders in the digital landscape.

The research showed that MMPs have strong data protection measures, with 100% implementing staff training, privacy policies, access controls, data audits and encryption. Additionally, 92.59% focus on customer consent management and appointing data protection officers (DPOs), while 85.19% use anonymisation techniques, showing a high commitment to safeguarding consumer data.

Figure 3

### Proactive risk mitigation measures employed by MMPs

Source: GSMA Mobile Money Regulatory Risk Management Survey

Training programmes for staff on data protection	100.00%
Development of data privacy policies and procedures	100.00%
Implementation of access controls and authentication mechanisms	100.00%
Regular data audits and compliance checks	100.00%
Data encryption and secure storage solutions	100.00%
Customer consent management and transparency initiatives	92.59%
Appointment of a DPO	92.59%
Use of anonymisation or pseudonymisation techniques	85.19%

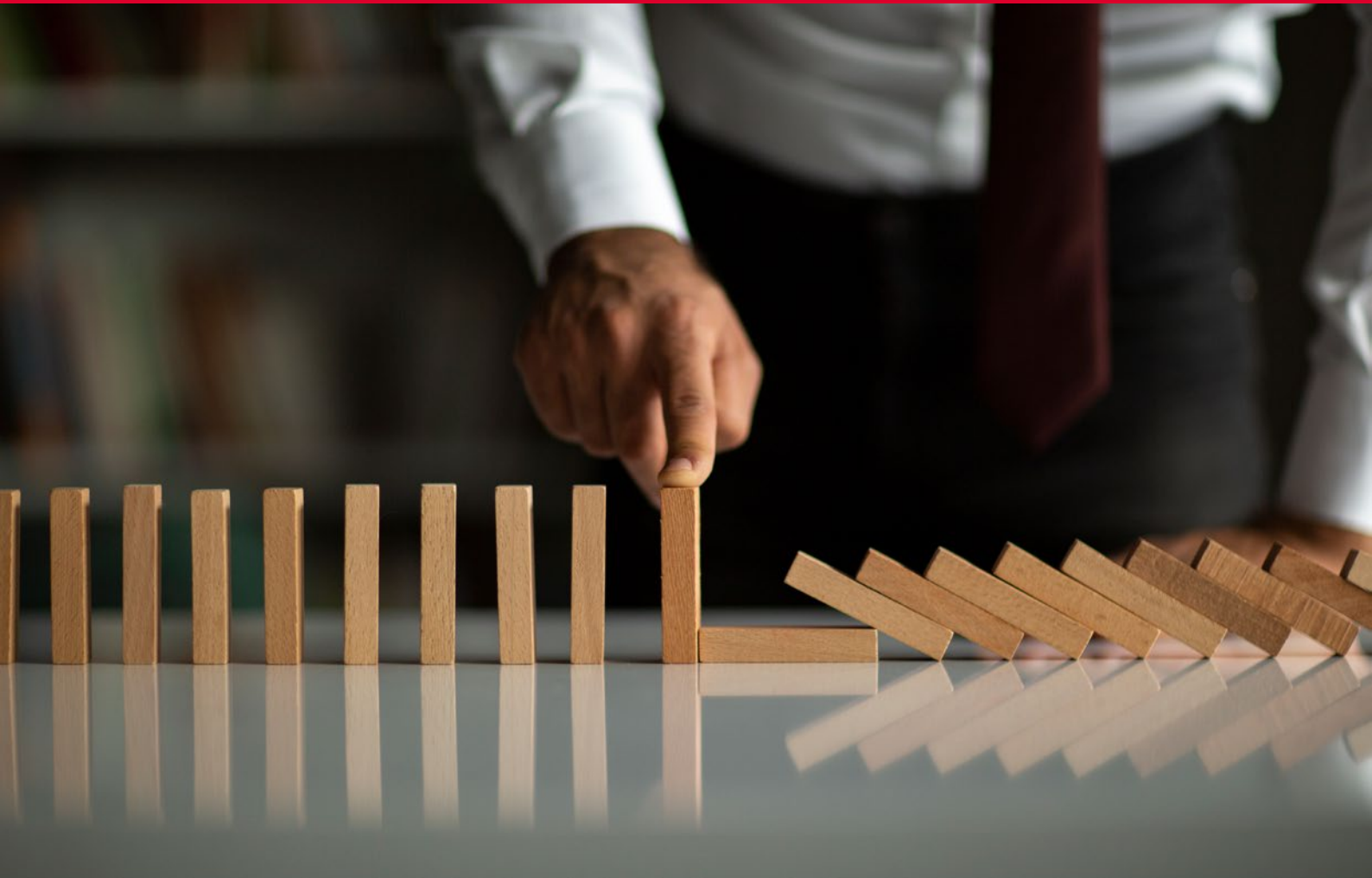
16 Republic of Kenya. (2019). *The Data Protection Act, 2019*.

17 Republic of Ghana. (2012) *Data Protection Act, 2012*.

18 Government of Nigeria. (2023). *Nigeria Data Protection Act, 2023*.

# 03

## Barriers to effective regulatory risk management



In the survey, 81.48% of respondents perceived regulations as slowing down technological advancements, indicating a critical gap in the regulatory framework governing digital finance. As innovations such as blockchain, AI and mobile payments evolve rapidly, existing regulations often fail to address the unique risks and challenges they pose. This creates uncertainty for businesses, which may hesitate to innovate without clear regulatory guidance.

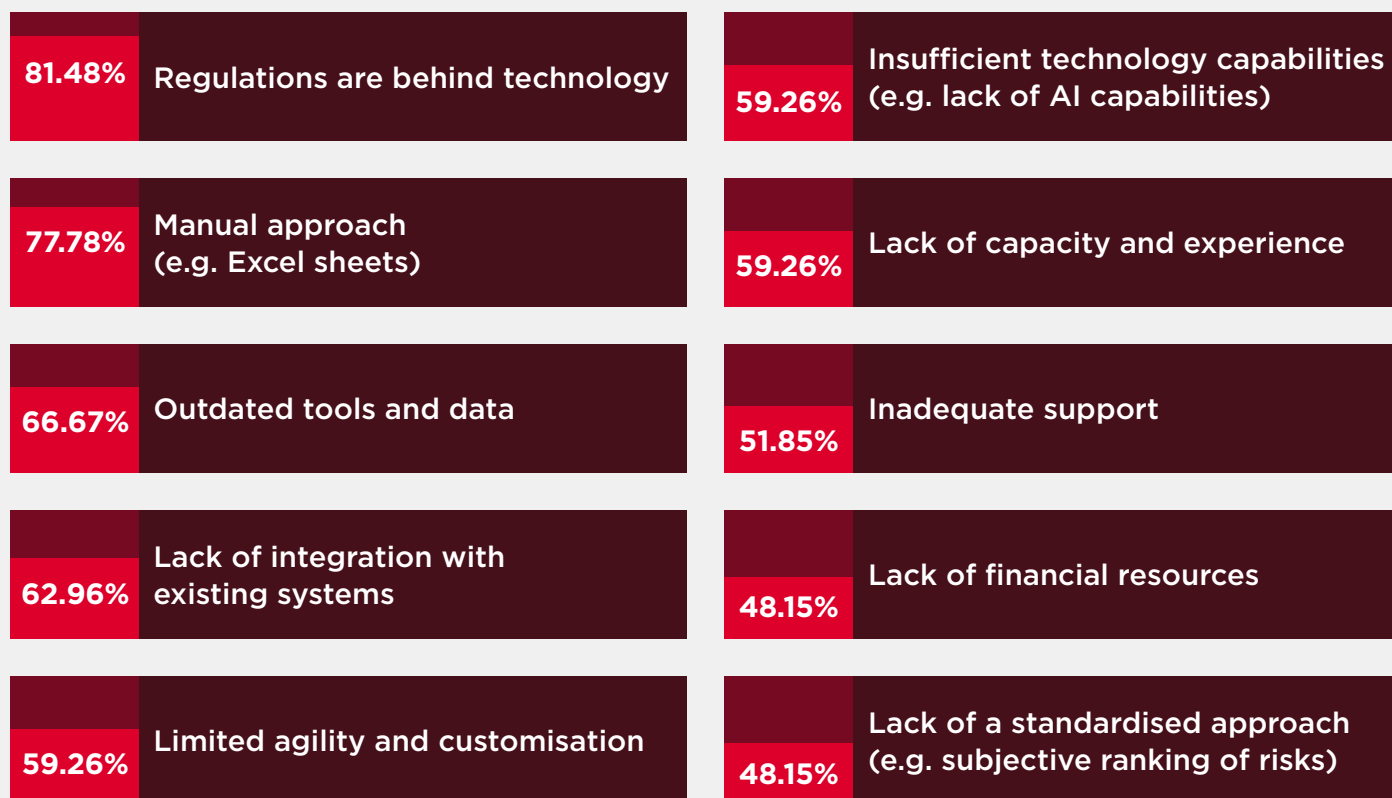
Survey respondents noted significant challenges in the mobile money sector, particularly regarding reliance on manual processes (77.78%) and outdated tools (66.67%). They emphasised that using manual methods, such as Excel for risk management, increases errors and slows response times. Additionally, legacy systems lack integration and advanced analytics, which hinders effective decision making.

The lack of integration in existing systems also poses a significant challenge in the mobile money sector, as noted by 62.96% of respondents. This issue leads to operational inefficiencies, data inconsistencies and poor customer experiences due to information silos. Figure 4 summarises the challenges identified in the sector.

Figure 4

## Summary of challenges identified in the mobile money sector

Source: GSMA Mobile Money Regulatory Risk Management Survey



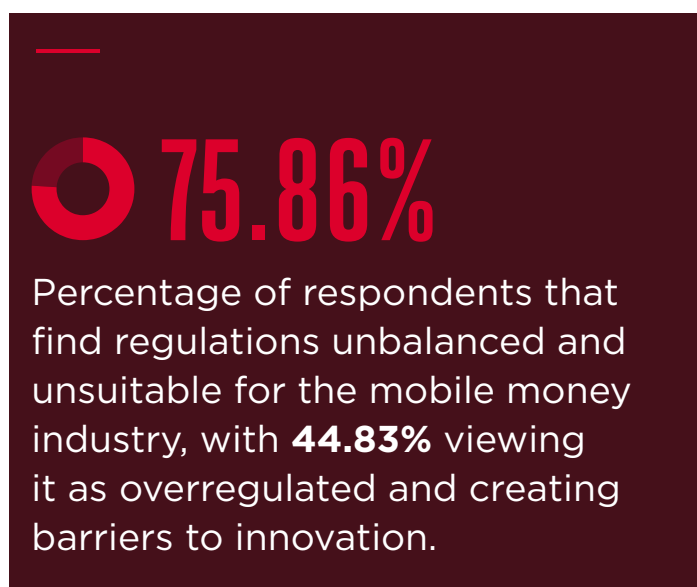
# 3.1

## Overregulation and uncertainty: the industry's double burden

Overregulation broadly refers to a situation in which regulations, laws, rules or government policies are perceived as excessively stringent, complex or unnecessary and have a number of negative impacts.

Overregulation and constant regulatory changes are frequently cited as barriers to business operations in the mobile money sector. In Kenya,<sup>19</sup> for example, stricter regulations introduced by the central bank in 2019 forced smaller MMPs to exit the market due to compliance costs. Regulatory environments in several African and South Asian countries were found to create barriers that hindered market entry and innovation.

Studies highlight that many countries have introduced stringent AML/CFT, KYC and consumer protection laws and regulations that significantly increase operational costs.<sup>20</sup> These measures are necessary but often burdensome, especially for small providers struggling to keep up with changing regulatory requirements. From the case studies, it was evident that many providers<sup>21,20</sup> had to continuously adjust their operational models to regulatory updates. These regulatory changes are often reactive, in response to fraud or market shifts and a lack long-term vision. For example, the implementation of enhanced KYC regulations in Nigeria necessitated system upgrades and increased staffing for compliance monitoring, driving up operational costs for smaller providers.



Studies highlight that most MMPs view regulatory compliance as an obstacle to business development.<sup>22</sup> Rather than fostering growth, regulations are often seen as a series of hurdles that require significant investment in compliance systems, limiting overall market agility and competitiveness.<sup>22</sup>

19 Ndwiga, D. (May 2020). *The Effects of Fintechs on Bank Market Power and Risk-Taking Behaviour in Kenya*. Kenya Bankers Association.

20 Meagher, P. (November 2017). *Regulatory Framework for Digital Financial Services in Côte d'Ivoire: A Diagnostic Study*. CGAP Working Paper.

21 Olayinka, D.W., Ihenichor, N. and Kelikume, I. (2018). *A Resource-Based View of Digital Financial Services (DFS): An Exploratory Study of Nigerian Providers*.

22 RADD. (n.d.). *The Future of Fintech: How Regulatory Challenges are Driving Innovation*.

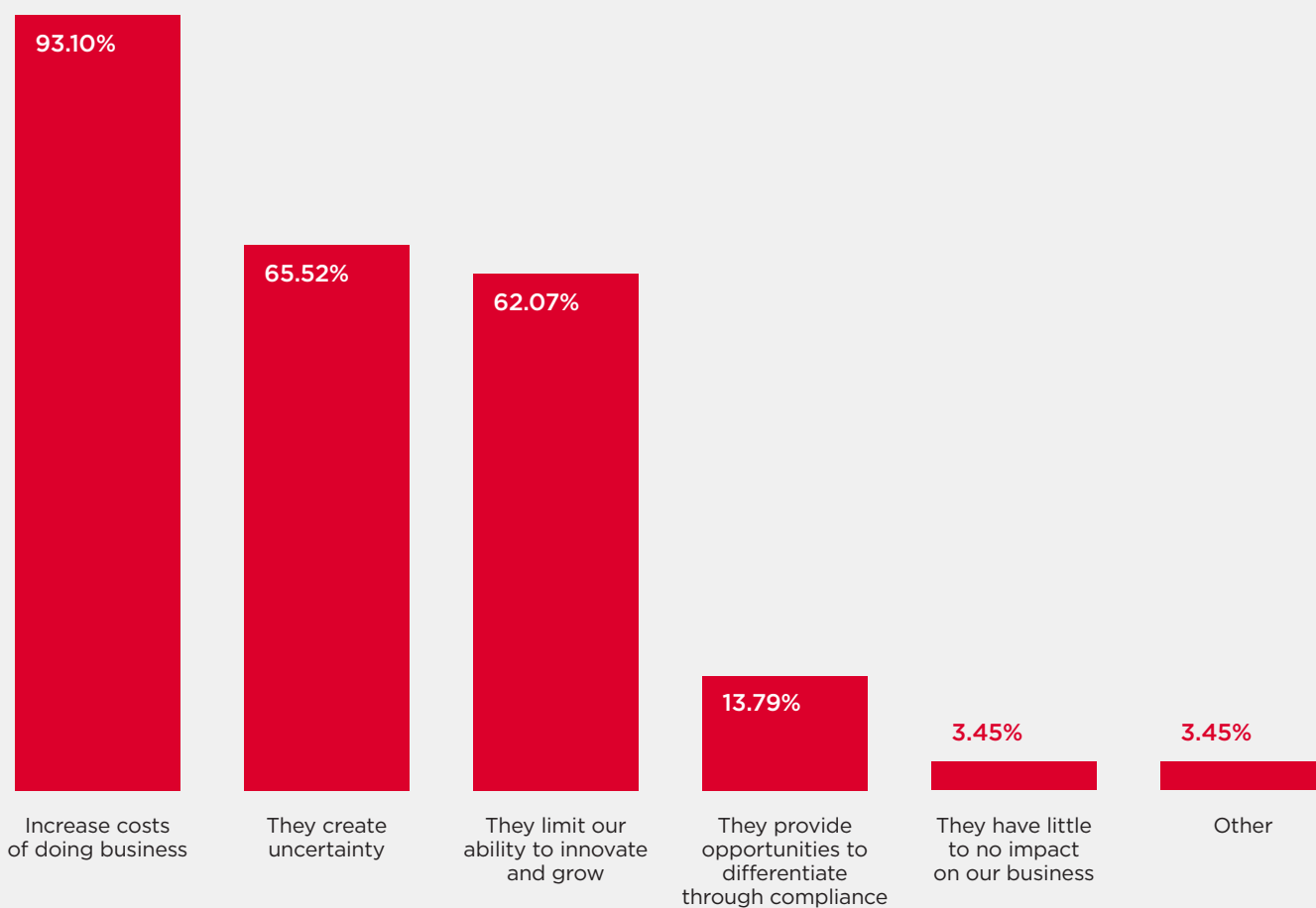
In the survey, 93.10% of respondents indicated that regulatory compliance increases the cost of doing business (Figure 5). Regulatory uncertainty also poses challenges for more than two-thirds of respondents, making it difficult to navigate the regulatory landscape.

Regulatory uncertainty is a significant challenge, with around two-thirds of respondents stating that it limits their ability to innovate. Providers are hesitant to invest in new technologies or expand services due to the constantly changing regulatory landscape, which creates uncertainty about future compliance requirements. More than half (57.62%) of respondents believe that regulatory changes have a significant impact on innovation.

Figure 5

## How regulatory issues affect business

Source: GSMA Mobile Money Regulatory Risk Management Survey



## 3.2

# Compliance challenges: a costly endeavour

One of the most significant challenges highlighted in the literature is the cost of compliance. Regulatory changes often necessitate investment in compliance infrastructure, such as advanced monitoring systems and staff training for AML/CFT and KYC protocols. For example, the Central Bank of Nigeria's (CBN) enhanced regulations on mobile money and e-payment systems in 2018 required providers to bolster their KYC and AML/CFT protocols, affecting operational efficiency and increasing costs.<sup>23</sup> Safaricom's M-PESA had to upgrade their AML/CFT systems significantly, implementing real-time transaction monitoring and reporting that increased operational complexity and costs.<sup>24</sup>



55.17%

of survey respondents reported financial losses, penalties or unforeseen expenses due to regulatory risks over the past three years. This finding correlates with the literature, which indicates that compliance costs are a major concern for DFS providers. One of the respondents reported average losses of \$100,000 annually.

<sup>23</sup> USAID. (2018). *The Digital Financial Services Landscape in Nigeria: Enabling Market Conditions For Pay-As-You-Go Solar*.

<sup>24</sup> Ndung'u, N.S. (2021). *A Digital Financial Services Revolution in Kenya: The M-PESA Case Study*.



# 04

## Case studies: navigating regulatory risks



# 4.1

## Strengthening Sri Lanka's AML/CFT framework and the need for higher transaction limits



Sri Lanka had various legal measures in place to deter money laundering, such as declaring large currency imports/exports and implementing KYC guidelines, but these measures were not sufficient to prevent money laundering.

Recognising the need for a robust AML/CFT regime, the government introduced The Prevention of Money Laundering Act, No. 5 of 2006, the Financial Transaction Reporting Act, No. 6 of 2006 and the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005, to provide a comprehensive legal framework.

Despite these measures, Sri Lanka was identified as a “grey list” country by the FATF in 2011 and 2017, respectively, with strategic deficiencies in its AML/CFT framework. Following the 2017 Mutual Evaluation by the FATF, the EU “blacklisted” Sri Lanka for noncompliance with international standards. In 2019, Sri Lanka was removed from the grey list after gaps in the legal and institutional framework were addressed. Sri Lanka’s third FATF Mutual Evaluation is scheduled for March 2025.

The Central Bank of Sri Lanka (CBSL), in collaboration with the national financial intelligence unit (FIU), is enforcing strict controls in the financial services industry to prevent future greylisting by the FATF. The National Policy on AML/CFT for 2023–2028 aims to strengthen the legal framework to combat money laundering by amending legislation, strengthening risk-based supervision of financial institutions, promoting domestic and international cooperation, boosting awareness of AML/CFT and developing comprehensive databases for better data management and security. The policy also aims to achieve inclusive financial integrity by promoting sustainable financial inclusion, enhancing financial literacy, expanding innovative product access, focussing on low-risk groups and adopting a simplified customer due diligence (CDD) framework to support low-risk financial inclusion efforts.

In interviews, MMPs highlighted actions that have had a positive impact on regulatory risk management, including:

- **Automation of AML/CFT and anti-fraud controls:** MMPs are increasingly implementing automated systems to efficiently monitor and mitigate risks related to money laundering, terrorist financing and fraud.
- **Enhanced collaboration:** Stronger partnerships between MMPs and the CBSL have fostered operational flexibility and better regulatory alignment, enabling more robust risk management.

Interviewees also highlighted the financial strain of stringent AML/CFT protocols on mobile money operations, particularly given low transaction limits and the fact that MMPs have the same AML/CFT and KYC requirements as banks. Maintaining compliance requires ongoing, intensive employee training to keep pace with changing regulatory standards and accurately identify suspicious activities. This high level of diligence incurs significant operational expenses, demanding robust systems and processes to ensure compliance.

Raising transaction limits would help MMPs offset these compliance costs, enabling them to pursue sustainable growth while meeting regulatory expectations.

## 4.2

# Strides in Ghana to boost digital finance despite challenges



The Bank of Ghana (BoG) has made significant progress in the development of regulations to support the growth of mobile money and DFS in Ghana, starting with the Payment Systems Act in 2003 and several other key laws, including the 2019 Payment Systems and Services Act (Act 987). These regulations have expanded participation and enabled innovation in the sector.

Major innovations like the GhQR code have improved the DFS regulatory framework and boosted consumer uptake of DFS in Ghana. In 2020, the GhQR had only 904 transactions totalling 98,336 GHS (about \$6,431). In 2022, there were 958,774 transactions with a value of GHS 638.6 million (about \$41,764,440).<sup>25,26</sup>

Still, there are regulatory gaps, such as data localisation laws that hinder cross-border services, unclear guidelines on cryptocurrencies and AI, potential price controls and taxation risks that affect affordability. The BoG is now working on eCedi, a digital currency, as part of their continued commitment to digital innovation.



The Ghana national Quick Response (GhQR) code, developed by the BoG and the Ghana Interbank Payment and Settlement Systems (GhIPSS), promotes financial inclusion by enabling cashless transactions for micro, small and medium-sized enterprises (MSMEs). However, it presents regulatory challenges related to data security and compliance with AML/CFT standards.

<sup>25</sup> Dowuona, S. (10 July 2023). "Universal GhQR - most secure, most affordable way to pay". *The B&FT Online*.

<sup>26</sup> Xe.com currency conversion rate as of 2 December 2024

# 4.3 Challenges and progress in Pakistan's financial inclusion and regulatory landscape



With more than 220 million people, Pakistan remains largely unbanked, with only 21% of adults financially included as per the Global Findex Database 2021. Efforts to increase inclusion began in the early 2000s with regulations supporting electronic transactions and branchless banking. The State Bank of Pakistan (SBP) also extends the support beyond the regulations where ideas or solutions affect the entire population, financially includes the unbanked population or has a positive impact on the financial industry. Recently, the SBP has enhanced efforts to create a supportive digital ecosystem and issued regulations for electronic money institutions, licensed new digital bank players and launched the RAAST instant payment system.

As of Q2 2024, 16 banks in Pakistan offer branchless banking services and encompass various technology-driven channels – such as banking agents, mobile and internet banking, ATMs, kiosks, and electronic money institutions – that enable financial service delivery without traditional branches. Together, these channels enhance accessibility and convenience, driving financial inclusion for the unbanked and underbanked populations.

Through interviews with several branchless banks in Pakistan, valuable insights into the regulatory opportunities emerged. These opportunities underscore the positive role of evolving regulations in strengthening branchless banking in Pakistan.

During the COVID-19 pandemic, financial institutions, including branchless banks, were directed to promote alternate delivery channels, such as online and mobile banking, and to waive fees on real-time gross settlement (RTGS) and interbank fund transfers (IBFTs) to help reduce COVID-19 transmission. Later, on 16 June 2021, the SBP allowed financial institutions to charge 0.1% or PKR 200 (whichever is lower) for transactions exceeding a monthly aggregate limit of PKR 25,000 per account. While intended to support cost recovery for digital fund transfer services, this disproportionately affects branchless banks, where average transactions are much smaller (around PKR 4,000 to 5,000), which means this limit affects a larger proportion of their transactions and clientele. This fee structure threatens the sustainability of branchless banks and their role in financial inclusion, underscoring the need for revisiting fee structure or providing targeted support.

Additionally, IBFTs are frequently exploited by agent networks, creating challenges for both branchless banks and customers. Agents often charge customers a cash deposit fee but bypass the standard process by transferring funds directly from their own accounts to the customer's account. This practice undermines the financial model of branchless bank providers, leading to significant revenue losses as they do not receive a share of the fee. Moreover, it unfairly burdens customers, who end up paying for what should be a free transaction for amounts under PKR 25,000. To address these challenges, a fair usage policy could be introduced to prevent agents from exploiting free transaction structures and ensure equitable cost recovery.

Pakistan's inflation index has surged significantly from 2008 to 2024 which reflects substantial cumulative inflation over the years, indicating a considerable reduction in purchasing power. However, transaction limits have not kept pace with inflation. In 2008, the daily transaction limit for Level 0 accounts was set at PKR 10,000, with an annual limit of PKR 120,000. By 2024, these limits have only marginally increased to PKR 25,000 per day and PKR 200,000 per year, respectively. This limited adjustment does not correspond with the fivefold increase in the inflation index, placing significant constraints on purchasing power and daily transactional capabilities for Level 0 customers. Furthermore, for biometric verification system (BVS)-verified accounts, the daily limit is slightly higher at Rs. 50,000, but these limits, which were introduced in 2019, have not been revised to reflect the inflationary changes. Revising these limits to reflect current economic realities is essential to support the continued growth of Pakistan's digital financial ecosystem.

Recognising this gap, the SBP has already exempted utility bill payments from being counted towards transaction limits. Building on this approach, exemptions for salary disbursements, loan disbursements, and repayments could further enhance the utility of branchless banking accounts. Such measures would not only provide greater transactional flexibility for users but also support the broader objectives of financial inclusion and economic empowerment.



# 4.4

## Kenya's digital finance framework



The regulatory landscape in Kenya is undergoing significant transformation. The Central Bank of Kenya (CBK), in collaboration with the World Bank, is working to review and update the 2014 regulatory framework to accommodate new market participants and technological advancements. The following are some of the notable strides in DFS in Kenya.

Kenya has been hailed for creating an open market that fosters innovation, with Safaricom's M-PESA a market leader in mobile money. However, some interviewees suggested that the telco-led model in Kenya may have contributed to a high number of mobile money fraud cases, without a clear regulatory framework for dealing with the issue. Laws such as the Computer Misuse and Cybercrimes Act, 2018 may not address the unique nature of mobile money fraud, which is characterised by low or fragmented fraud losses per victim and distance between victim and perpetrator (no face-to-face interaction). There is also a lack of government-driven identity verification solutions, such as biometric authentication (fingerprints, facial recognition or iris scans), which are more effective for customer registration and authentication.

In 2010, Kenya was first grey-listed by the FATF due to delays in implementing the Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), exposing gaps in its AML/CFT framework. Although legislative reforms and enhanced enforcement measures, including strengthening the Financial Reporting Centre and Asset Recovery Agency, led to its removal from the grey list in 2014, Kenya faced renewed challenges. On 23 February 2024, the FATF grey-listed Kenya again, citing persistent weaknesses in enforcement, regulatory oversight and vulnerabilities in its financial system, highlighting ongoing struggles to combat financial crimes and bolster global confidence.

### KYC compliance

In 2022, the Communications Authority of Kenya mandated all telcos to run a country-wide KYC campaign to update customer details. Plans are underway to adopt digital KYC using biometric technology and the national ID database for improved identity verification.

### Collaboration

Cooperation between DFS providers, MMPs and regulators is improving, with a focus on developing regulatory frameworks and conducting fraud awareness campaigns.

## 4.5

# Nigeria's regulatory framework and the impact on risks



In Nigeria, the Mobile Money Regulatory Framework (2015) and Payment Services Bank (PSB) licensing model allow MNOs such as MTN to operate in the financial space. Despite a strong regulatory environment and consumer protection controls due to a bank-led model, mobile money in Nigeria could be perceived as overregulated and hindering innovation. In addition, some argue that the bank-led model does not manage risks better.

For instance, fraud is still on the rise in Nigeria's Inter-Bank Settlement System Plc (NIBSS), which is owned by all licensed banks, including the CBN. In 2023, there was a reported 112% increase in fraud, with data indicating a steady increase every year.<sup>27</sup> The country's tiered KYC regulation is, however, hailed as a positive step towards digital inclusion and proportional regulations.

## 4.6

# Mandatory biometric SIM card registration in Tanzania for KYC



In 2018, the Tanzanian government began implementing a biometric SIM card registration programme to curb identity fraud and SIM swap crimes. Managed by the Tanzania Communications Regulatory Authority (TCRA), this initiative requires all mobile users to re-register their SIM cards using biometric identifiers, primarily fingerprints. The move aimed to create a secure digital identity system that connects each mobile subscriber's SIM card to their unique ID issued by the National Identification Authority (NIDA), thereby reducing fraudulent activities that exploit anonymous SIM ownership.

One of the key results of this programme was a substantial reduction in SIM-related fraud, with some reports citing up to a 90% decrease in identity theft cases involving SIM swaps.<sup>28</sup> However, the programme has faced some challenges, particularly around data privacy concerns, as Tanzania lacks comprehensive data protection laws.<sup>29</sup> Additionally, the requirement for citizens to obtain a NIDA ID for SIM registration presents obstacles, as many do not possess mandatory documents like birth certificates. To address these issues, the TCRA has launched nationwide campaigns, including outreach and social media influencer partnerships, to encourage compliance and streamline registration processes.

27 NIBSS. (2024). *Annual fraud landscape: Jan-Dec 2023*.

28 GSMA. (2024). *Mobile money fraud typologies and mitigation strategies*.

29 Biometric Update. (4 July 2023). "Report finds data protection loopholes in Tanzania's biometric SIM registration drive". *BiometricUpdate.com*.

# 4.7

## Other regulatory risk mitigation initiatives

Other initiatives have been undertaken by regulators to mitigate the regulatory risks associated with mobile money. Many regulators require strict licensing and operational oversight for MMPs to reduce the risk of noncompliance. In countries such as Pakistan, MMPs need to follow strict KYC and AML/CFT protocols.<sup>30</sup>

Regulators often encourage or mandate interoperability between mobile money platforms to mitigate risks associated with fragmentation. This ensures that mobile money users can transfer funds across different platforms safely, reducing systemic risks and enhancing financial inclusion.<sup>31</sup>

Many African countries are implementing data protection laws to mitigate data privacy risks. For example, Kenya's Data Protection Act 2019 provides a comprehensive framework for protecting personal data. The law, enforced by the Office of the Data Protection Commissioner (ODPC), outlines strict requirements for the collection, processing and security of personal data, similar to global standards. In Pakistan, the SBP has established specific regulations for MMPs with their *Rules for Payment System Operators and Payment Service Providers*. These guidelines outline operational requirements for compliance and risk mitigation in the mobile money sector.<sup>32</sup>

---

<sup>30</sup> FATF (March 2020). *Guidance on Digital Identity*, p. 24.

<sup>31</sup> GSMA. (2016). *The Impact of Mobile Money Interoperability on Financial Inclusion: Evidence from five country case studies*, p. 8.

<sup>32</sup> State Bank of Pakistan. (2020). *Rules for Payment System Operators and Payment Service Providers*, Version 2.0, Chapter 4.



# 05 Structured approach to regulatory risk management



The literature reviewed suggests that full regulatory compliance gives MMPs a competitive edge<sup>33</sup> by building consumer trust and reducing penalties. The survey showed a strong commitment to compliance and staying ahead of regulations,<sup>34</sup> with 72.41% of survey respondents reporting they are fully aligned with current regulations and 75.86% having formal compliance strategies.

This maturing compliance framework highlights the importance of proactive risk management for sustainable growth and operational stability, with providers prioritising regulatory alignment to minimise risks and maintain their competitiveness in dynamic markets.<sup>35</sup>

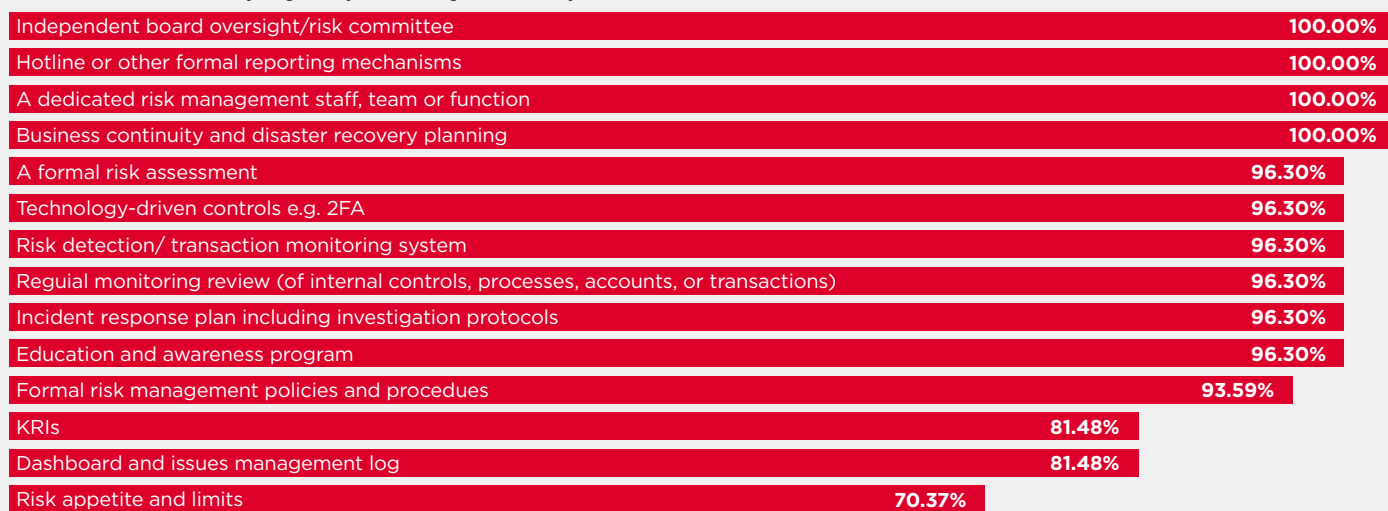
In the survey, all respondents confirmed they have a risk management framework in place, indicating that MMPs recognise the importance of formal risk management in navigating complex and changing regulatory environments. The survey findings also suggest that mobile money and other DFS providers have implemented several key risk management practices, as illustrated in Figure 6.



Figure 6

## Risk management practices in place

Source: GSMA Mobile Money Regulatory Risk Management Survey



33 World Bank Group and ASEAN. (March 2019). *Advancing Digital Financial Inclusion in ASEAN: Policy and Regulatory Enablers*.

34 Sefrina, M. (March 2024). *An Inclusive Digital Economy in the ASEAN Region*. ERIA Discussion Paper Series, No. 505.

35 Ochen, R. and Nsubuga Bulime, E.W. (May 2023). *Digital Financial Services Regulations: Their Evolution and Impact on Financial Inclusion in East Africa*. KBA Centre for Research on Financial Markets and Policy Working Paper Series.

Effective risk management involves multiple strategies that work together. Independent board oversight and dedicated risk management teams provide governance and expertise, while formal reporting mechanisms encourage transparency and early risk detection. Business continuity and disaster recovery plans safeguard operations during disruptions and regular risk assessments prioritise the most significant threats. Technology-driven controls such as two-factor authentication strengthen security, while risk detection systems and internal control reviews ensure continuous monitoring and compliance. Incident response plans minimise damage from breaches and education programmes foster a risk-aware culture.

“Risk culture” refers to the values, beliefs, attitudes and behaviours within an organisation that shape how employees and leadership perceive, understand and manage risks. A strong risk culture promotes proactive risk management and aligns with the organisation’s goals and risk appetite, ensuring that risk considerations are embedded in day-to-day decision-making at all levels. Key aspects of risk culture include leadership from the top, accountability and ownership, communication and transparency, risk awareness and education. It should be clear through training and awareness-raising programmes that risk management is everyone’s responsibility and that staff should take ownership of risks in their area.










Formal risk management policies provide consistency, with key risk indicators (KRIs) offering early warnings for proactive mitigation. Dashboards and issue logs track risks in real time and clearly defined risk appetites ensure decisions are aligned with strategic goals and acceptable risk levels. Together, these strategies create a robust framework for managing risks.

As indicated in the survey results, risk appetite and limits, as well as KRIs, were among the least-used risk management practices among MMPs. Dashboards and issue logs, which are tools for monitoring risks, were also the least employed. These practices are linked to KRIs since dashboards monitor KRI matrices to track deviations from set limits in line with the risk appetite.

“Risk appetite” is the amount and type of risk an organisation is willing to accept in pursuit of its objectives. It is important that the board sets rules for all types of risk. Risk appetite translates into a set of procedures that ensure risk receives adequate attention in decision-making and ultimately dictates operational constraints for routine activities. These constraints can then be translated into KRIs and monitored actively. Table 2 provides examples for MMPs.

Table 2

## Examples of qualitative and quantitative risk measures

Type of measure	Quantitative examples	Qualitative examples	Key Risk Indicators (KRIs)
 <b>Strategic</b>	Customer base expansion: Achieve 10% quarterly growth in user base in existing markets	Focus on customer retention in established markets while expanding strategically	Decline in customer acquisition: Alert if quarterly growth falls below 5%
 <b>Regulatory</b>	License compliance: 100% adherence to licensing requirements in each operating country	Strong emphasis on regulatory compliance across jurisdictions	Instances of licence non-compliance: Target 0 annually
 <b>Financial</b>	Exposure limits: Cap on outstanding microloans at 20% of total assets	Conservative approach to high-risk credit offerings	Default rate on loans: Target <3% on mobile lending portfolio
 <b>Operational</b>	Daily transaction volume: Max \$1M daily across all agents	Avoid exceeding 90% capacity to ensure system stability	Number of transactions nearing daily limit: Alert at 80% threshold
 <b>Third party</b>	Liquidity requirements for agents: Min 50% of daily transaction volume	Flexible stance on regional cash requirements	Agent liquidity levels below threshold: <5% of agents monthly
 <b>Technology</b>	System uptime: Minimum 99.9% uptime to ensure continuous access	Strong commitment to operational resilience and system reliability	System downtime events: Track downtime >10 minutes per month
 <b>Fraud</b>	Fraud detection rate: Target >95% detection of fraudulent transactions	Proactive in adopting advanced fraud prevention tools	Unresolved fraud alerts: Target 0 unresolved monthly
 <b>Operational</b>	Transaction error rate: Target <0.1% of transactions	Focused on minimising customer impact through error prevention	Frequency of transaction errors: Alert at 0.05% increase monthly
 <b>Reputation</b>	Customer complaint resolution rate: Resolve 98% of complaints within 24 hours	Zero tolerance for unresolved customer complaints beyond 48 hours	Volume of unresolved customer complaints: Monthly target <1% of total complaints

# 5.1

## Risk assessment tools

Regular risk assessments are crucial to maintain compliance with changing regulatory requirements. For instance, MMPs in Kenya<sup>36</sup> and Ghana<sup>37</sup> frequently perform risk assessments to monitor compliance with AML/CFT regulations, data privacy laws and cybersecurity standards.

Nearly all survey respondents – 96.55% – stated they have clear risk scoring, analysis and evaluation criteria in place. These tools enable MMPs to analyse and evaluate risks by assigning high, medium and low scores to the likelihood and impact of risk. However, as observed in many of these scoring guidelines, there are no clear or less subjective quantitative and qualitative measures to determine a score. For instance, the *Digital Financial Services and Risk Management Handbook* contains qualitative probability and impact ratings of 1 to 5, but it is not clear what factors should be considered when selecting a score.<sup>38</sup> The GSMA recommends the following tools for MMPs to enhance their risk assessments.

---

### Impact measurement guide

In risk management, “impact” refers to the consequences or effects that a risk event could have on an organisation’s objectives. As mentioned in [Section 1](#), reputational risk is a consequential risk that can be assessed as an impact. Financial impact is easier to measure as it is based on financial figures.

Table 3 provides an example of an impact measurement guide. Please note that the measures are for illustrative purposes only. This risk impact measurement guide assesses financial, reputational and regulatory/legal impacts across five levels, from “Insignificant” to “Severe”. Each level specifies the potential consequences in these areas:

- **Financial impact:** Ranges from losses exceeding \$1,000,001.00 (Severe) to less than \$5,000 (Insignificant), with each level indicating a lower financial impact.
- **Reputational impact:** Measures the extent of negative publicity and confidence disruption, from widespread international scrutiny and severe market reaction (Severe) to minimal or unlikely effects (Insignificant).
- **Regulatory and legal impact:** Evaluates the potential for regulatory scrutiny or legal consequences, from significant legal actions or regulatory sanctions (Severe) to negligible regulatory concern (Insignificant).

This structure allows organisations to assess the impact of risks comprehensively and prioritise risks based on their financial, reputational and regulatory/legal consequences.

---

<sup>36</sup> Republic of Kenya. (October 2021). *Money Laundering and Terrorism Financing National Risk Assessment Report*.

<sup>37</sup> Alliance for Financial Inclusion (AFI) (2023). *The Supervision of FinTech in The Africa region: A Case Study of Ghana*.

<sup>38</sup> IFC World Bank Group. (2016). *Digital Financial Services and Risk Management Handbook*.

Table 3

## Example of an impact measurement guide

Rating	5 Severe	4 Major	3 Moderate	2 Minor	1 Insignificant
<b>Financial</b>	X > \$1,000,001	X \$250,001 -\$1,000,000	X \$100,001 -\$250,000	X \$5,001 -\$100,000	X < \$5,000
<b>Regulatory and legal</b>	<ul style="list-style-type: none"> <li>Product withdrawal, non-approval of major product or forced closure of major operations, function, business line or branch.</li> <li>Potential criminal prosecution, very high fines and/or executive officer imprisonment or debarment</li> <li>Prolonged, extensive litigation</li> </ul>	<ul style="list-style-type: none"> <li>Agency scrutiny</li> <li>Regulators may make a for-cause visit to bank</li> <li>Lack of confidence in one or more elements of local management system</li> <li>Allegation of serious breach of regulation with investigation or report to authority with potential for significant fines</li> </ul>	<ul style="list-style-type: none"> <li>Short-term agency scrutiny. Requires notification to or involvement of regulators</li> <li>Limited legal issues (e.g. individual civil action) with moderate monetary damages</li> </ul>	<ul style="list-style-type: none"> <li>Limited regulatory implications</li> <li>Regulators request clarity around issue</li> <li>Possible legal challenge with modest out-of-court settlement</li> </ul>	<ul style="list-style-type: none"> <li>Unlikely/rare regulatory implications</li> <li>Unlikely/rare to encounter legal challenge</li> </ul>
<b>Reputational</b>	<ul style="list-style-type: none"> <li>International media scrutiny or extensive national coverage.</li> <li>Long-term disruption of stakeholder and customer confidence</li> <li>Severe market reaction anticipated</li> </ul>	<ul style="list-style-type: none"> <li>Mid-term national coverage and limited mainstream media coverage</li> <li>Adverse publicity to customer</li> <li>Significant damage to reputation/image</li> </ul>	<ul style="list-style-type: none"> <li>Short-term media coverage, localised concern/complaints, especially from non-mainstream sources</li> <li>Short-term effect on reputation</li> </ul>	<ul style="list-style-type: none"> <li>Limited negative publicity e.g. customer complaint on social media or at branch that may generate a few mentions/retweets</li> </ul>	<ul style="list-style-type: none"> <li>Unlikely effect on reputation/image</li> </ul>

### Calculating the impact score

The three parameters – financial, regulatory and legal and reputational risks – can then be weighted and one impact score obtained to multiply with the selected likelihood score.

For instance, if a fraud risk like identity theft was scored 4 for financial, 3 for regulatory and Legal and 2 for reputational, the weighted impact score will be 3 and calculated as  $(4+3+2)/3$ , giving an impact score of 3.




Table 4

## Example of a likelihood guide

Rating	Description	Guidance
5	<b>Almost certain</b>	A significant number of incidents are likely to occur weekly
4	<b>Likely</b>	Incidents are expected to happen monthly
3	<b>Possible</b>	An incident may occur approximately once every quarter
2	<b>Unlikely</b>	Incidents might happen occasionally, perhaps once a year
1	<b>Rare</b>	Incidents are unlikely to occur within a year but may happen over a longer time frame

Table 5

## Risk score guide

Colour code	Risk score range	Level	Description
	25-12	<b>High</b>	High risks should immediately be brought to senior management attention and actively managed to lower levels. Appropriate resources should be urgently deployed.
	12-9	<b>Medium</b>	Review your existing control measures and add whatever Additional Control Measures may be necessary to bring the risk back to a Low or Minimal risk
	9-0	<b>Low</b>	Minimal resources and attention, however continuously monitor to ensure they do not move to medium or high

## Likelihood assessment guide

In risk management, “likelihood” refers to the probability or chance that a risk event will occur. It is a key factor in assessing and prioritising risks, as it helps organisations understand how probable certain risks are relative to others. Table 4 provides an example of a likelihood guide. Please note that the measures under the guidance column are for illustrative purposes only.

## Risk scoring guide

Regulatory risk scoring solutions from regtech providers can assist in risk scoring based on compliance factors such as AML/CFT, KYC, regional regulations and data protection laws using unstructured data. These tools can enable organisations to proactively identify high-risk areas, allowing them to manage regulatory risks effectively. For example, MMPs could integrate, for instance, the Central Bank of Kenya’s risk-based supervision framework with factors such as AML/CFT and KYC compliance, data protection and consumer protection standards.

## Calculating the risk score

After calculating the impact score, the risk score can be calculated by multiplying the impact score with the likelihood rating. Using the previous example, if the same fraud risk – identity theft – was rated 4 (Likely) based on previous incidents or consultations in workshops and brainstorming sessions, then the risk score would be 12 (3×4). The risk score guide is shown in Table 5.

This particular risk score, 12, would fall under Medium risk. Once all risks are analysed and evaluated, they are ranked in order of priority from the highest score to the lowest. This will inform the risk treatment strategy to accept, transfer, avoid or control (ATAC) priority risks, ensuring they are managed effectively. A separate, comprehensive toolkit is provided as an addendum to this report for this risk assessment process.

# 5.2

## Risk management tools

The standard systems used for regulatory risk management include transaction monitoring systems and other related systems, such as fraud management systems (FMS). However, studies show that these tools can be ineffective as most rely on rule-based detection methods.

---

### Regtech solutions

Regulatory technology (regtech) solutions often integrate AI and machine learning to detect suspicious patterns and anomalies in real-time. These tools identify potential fraud or money laundering activities with greater precision, reducing false positives and enabling quick responses.

According to Juniper Research (2022), the global regulation technology is estimated to spend over \$204 billion by 2026, accounting for 50% of all regulatory compliance spend for the first time given the scale of the regulatory burden facing the financial services industry.

Regtech providers additionally enable organisations to reduce regulatory risks by streamlining and automating compliance processes without significant investment in in-house systems. Regtech automates repetitive tasks like AML/CFT checks, KYC verification and transaction monitoring. This enables MMPs to meet regulatory requirements while controlling costs.

Lastly, regtech solutions are designed to adapt to evolving regulatory landscapes. They update compliance frameworks dynamically, helping businesses stay aligned with new laws and guidelines without significant operational disruption. By integrating regtech, MMPs can proactively manage regulatory risks, improve operational efficiency and build trust with regulators and consumers alike.

---

## Regulatory sandboxes

Regulatory sandboxes allow DFS providers, including MMPs, to test solutions in a controlled environment under regulatory supervision. This enables MMPs to reduce regulatory risks by ensuring that new products comply with local regulations before they are launched. Early collaboration with regulators through sandboxes also fosters understanding of compliance requirements, allowing innovation to thrive while minimising the risk of noncompliance and without compromising financial stability.

The Monetary Authority of Singapore (MAS) has established one of the most notable regulatory sandboxes, with DFS players testing innovative solutions such as blockchain-based remittance services to ensure compliance with cross-border transaction regulations.

Alibaba Cloud, together with the Philippines' FinTech Alliance.ph, announced the launch of the Fintech Industry Sandbox Program, in support of Bangko Sentral ng Pilipinas (BSP), the Philippines' central bank. The objective of the sandbox programme is to support emerging digital technologies and address current challenges in the financial industry. For example, Alibaba Cloud provides a mix of fintech solutions to GCash, a leading MMP, to handle large volumes of digital transactions with minimal interruption and high cost efficiency.

---

## Cloud-based compliance solutions

Cloud-based, mobile-friendly compliance solutions improve scalability, cost-efficiency and accessibility, particularly for remote or underserved areas. By implementing real-time monitoring tools and using cloud platforms for regulatory reporting, organisations can reduce infrastructure costs and ensure compliance in regions with limited resources. This enables a streamlined, responsive compliance framework that adapts to changing regulatory demands. In India, the State Bank of India (SBI) has implemented cloud-based compliance and reporting tools to support rural branches and microbranches in remote locations. These cloud solutions improve scalability and allow real-time reporting, enhancing regulatory compliance in areas with limited digital infrastructure. This approach has reduced costs and improved accessibility, enabling better regulatory reporting and compliance for underserved populations.



**06**  
**Conclusion**



# Conclusion

---

Mobile money services have reshaped global financial inclusion, especially in Africa and South Asia, but have also introduced new risks, such as fraud, money laundering and cybersecurity threats.

For example, the rapid expansion of mobile money services in Sub-Saharan Africa has resulted in increased cases of fraud, where fraudsters exploit gaps in regulatory oversight or user education. Additionally, the lack of robust cybersecurity systems in some regions has made mobile money platforms vulnerable to hacking.

---

A one-size-fits-all approach to regulation may not be practical or effective, especially given the diverse nature of mobile money services.

Compliance with AML/CFT, KYC and data protection regulations is crucial for the integrity of mobile money services. However, regulations are often tailored to the scale, customer type and activities of the services to ensure effectiveness and proportionality. A practical example of such tailored regulation is seen in India, where the Reserve Bank of India (RBI) has implemented separate guidelines for prepaid payment instruments (PPIs). These guidelines distinguish between small PPIs and full KYC PPIs, with different regulatory requirements regarding the transaction limits and the level of customer verification. This distinction allows for differentiated compliance obligations depending on the scope and risk associated with the service.

---

Mobile money services vary greatly across regions in terms of adoption and maturity.

In Sub-Saharan Africa, services like M-PESA in Kenya have been around for over a decade and are well integrated into daily life. In contrast, in other regions like Southeast Asia or Latin America, mobile money is still in the early stages of growth, with lower penetration and slower adoption. These varying maturity levels result in distinct regulatory and operational risks that must be tailored to local needs.

---

The findings of the regulatory risk survey underscore growing consensus among MMPs about the value of structured risk management frameworks.

These frameworks, encompassing risk appetite definitions, KRIs and regular risk assessments, strengthen resilience to potential disruptions. The adoption of sophisticated risk detection tools and continuous monitoring mechanisms represents a shift towards a proactive and data-driven approach to risk management. Such advancements in regulatory compliance and risk practices enable MMPs to address both current and future regulatory challenges, fostering a risk-aware culture throughout their organisations. As MMPs align their operations with regulatory standards, they not only strengthen compliance, but also bolster their market competitiveness and reputation in a dynamic regulatory landscape.

---

The commitment of the mobile money industry is reflected in survey data indicating that 72.41% of respondents are fully compliant with current regulations, and 75.86% have implemented formal compliance strategies.

This signifies a strategic shift towards not only meeting regulatory requirements, but also staying ahead of regulatory trends.

---

The case studies in the report show the critical regulatory and operational developments in mobile money across several countries, emphasising enhanced AML/CFT frameworks, rising compliance costs and tailored risk mitigation strategies.

Sri Lanka's successful removal from the FATF grey list in 2019 highlighted progress in addressing AML/CFT deficiencies, although MMPs still face challenges with compliance costs and low transaction limits. Pakistan's branchless banking initiatives are improving financial access, yet lower transaction limits and regulatory restrictions on pricing affect sector growth. Kenya's evolving regulatory framework aims to address emerging fraud risks, while Tanzania's biometric SIM registration demonstrates significant fraud reduction despite data privacy concerns. Regionally, initiatives mandating interoperability and the implementation of robust data protection laws, such as Kenya's Data Protection Act, emphasise a commitment to systemic safety and compliance. Collectively, these insights reflect a focussed approach to regulatory risk management, supporting secure and inclusive growth of mobile money.

---

The report also outlined a mobile-money-specific risk typology, including categories such as fraud, technology, ESG and reputational risks.

For example, in mobile money, fraud and technology risks are elevated to primary risk categories due to their significant impact on operations and consumer trust. This interconnected typology illustrates how failures in one risk category, such as technology (cybersecurity threats), can amplify others, such as fraud, resulting in reputational harm.

---

The report also emphasises that mobile money growth and regulatory compliance must advance together to protect the sector from risks without limiting its potential to foster financial inclusion.

Technology-driven advancements such as AI-driven fraud detection, regtech and cloud-based compliance solutions offer MMPs the tools to manage regulatory risks more effectively. As mobile money becomes increasingly integral to financial ecosystems, it will be crucial for regulators and providers to collaborate, adapt and innovate to ensure a balanced approach that upholds consumer protection while allowing for sustainable growth.

---

The following section (Section 7) presents key recommendations to address the challenges and solutions identified in the research.

# 07 Recommendations



# Recommendations

---

To address regulatory challenges in the mobile money industry, a collaborative approach among providers, industry associations and regulators is vital to foster innovation and ensure consumer protection.

The rapidly evolving nature of financial technologies often outpaces existing regulatory frameworks, creating a need for mechanisms that can balance innovation with compliance. Strengthening partnerships between these stakeholders allows for open dialogue, shared learning and the co-creation of solutions tailored to local contexts and consumer needs. These partnerships are critical in addressing barriers such as inadequate regulations, operational risks and concerns around data privacy and security. In 2016, PayMaya Philippines Inc. announced that it has successfully conducted mobile money interoperability trials between its digital payments mobile app PayMaya with Globe Telecom's GCash, as part of a GSMA initiative to make mobile money services more inclusive and accessible, particularly among those without access to banking services. This was the first successful interoperability trial in Southeast Asia between two MMPs.

---

MMPs should consider investing in regtech and AI-driven compliance tools to streamline processes and enhance security.

Regtech automates key tasks, such as AML/CFT and KYC checks, and AI-driven fraud detection tools identify suspicious patterns more accurately, reducing false positives. Cloud-based compliance solutions improve scalability and accessibility, enabling providers in low-infrastructure areas to maintain regulatory standards efficiently. For example, Safaricom's M-PESA has implemented advanced AI-driven fraud detection systems to proactively counteract evolving threats in real-time and analyse user behaviors to identify anomalies and issue automated responses at scale. GCash, on the other hand, partnered with Alibaba Cloud and adopted a mix of solutions including infrastructure as a service, a cloud computing model, along with sophisticated security products to boost its ability to scale infrastructure in real time and intelligently defend their applications from any type of cyber vulnerabilities.

---

## Regulators should tailor AML/CFT and KYC requirements to meet the unique challenges of low-literacy and low-infrastructure environments, enabling MMPs to enhance financial inclusion without compromising compliance.

Implementing solutions like biometric verification and tiered KYC processes address barriers faced by underserved populations, particularly in rural and remote areas. Biometric systems, such as fingerprint recognition, offer a reliable and user-friendly way to verify identities, while tiered KYC frameworks allow for simplified compliance requirements for low-risk customers. These tailored measures not only ensure adherence to AML/CFT regulations but also facilitate the onboarding of individuals previously excluded from formal financial systems. In Nigeria, MMP Paga uses biometric verification, such as fingerprint recognition, and simplified KYC processes for low-risk customers in rural areas, successfully onboarding underserved populations while ensuring compliance with AML/CFT and KYC regulations.

---

## Cultivating a proactive risk culture within MMPs is vital in a dynamic regulatory landscape.

Leadership should embed risk awareness in decision-making and conduct regular risk assessments, using quantitative scoring where possible. Defining risk appetites, limits and KRIs enhances organisational resilience, preparing MMPs for regulatory changes. A prime example is Telesom, which, despite having no specific e-money regulation when it was launched in 2009, proactively implemented customer due diligence (CDD) procedures in line with FATF guidelines to mitigate the risk of financial crime.

---

## Given the reliance on external vendors and agents, comprehensive third-party risk management is essential.

Effective oversight should include due diligence, contractual safeguards and continuous training, particularly regarding fraud trends. Monitoring KRIs like system uptime helps ensure third-party services remain within acceptable risk levels. Contingency planning for essential services maintains continuity if external providers experience disruptions, particularly in IT support or transaction processing. When M-PESA was launched in Kenya, the system was initially built based on optimistic but realistic forecasts. However, the rapid success of the service far exceeded the initial forecasts and the technology struggled to keep up with the huge transaction volume, causing delays and system breakdowns. A task force was set up to rapidly increase capacity, but the process incurred significant costs due to the undersized launch system. This highlights the importance of third-party oversight programme, ensuring scalability, flexibility and effective risk management.

---

## MMPs should consider adopting open API platforms to mitigate regulatory risks arising from failed or suboptimal integrations with third-party partners.

While integrating with external entities is essential for expanding service offerings and enhancing customer experience, poor or incomplete integrations can lead to compliance failures, operational inefficiencies and even exposure to financial crime risks, all of which can attract regulatory scrutiny. For example, MTN's MoMo launched an open API programme to ensure that the partners are onboarded through a standardised, automated process that can be monitored and controlled for regulatory compliance.

---

## Real-time, localised fraud and AML monitoring solutions should be leveraged for detecting region-specific risks.

These tools are particularly effective in environments characterised by frequent, small-value transactions, which can be vulnerable to fraud and financial crimes. By tailoring monitoring systems to local transaction patterns and leveraging advanced technologies such as AI and machine learning, providers can detect anomalies with precision and mitigate risks proactively. Such systems not only enhance fraud detection capabilities but also ensure compliance with stringent AML/CFT regulations, fostering trust and confidence among users and regulators alike. M-PESA uses real-time fraud detection tools customised to monitor local transaction patterns. With frequent and often small transactions, M-PESA's localised monitoring system flags unusual patterns promptly, reducing fraud risks while complying with AML/CFT regulations. The system uses machine learning algorithms to enhance fraud detection, safeguarding the platform and ensuring trust among users.

---

## Blockchain technology should be leveraged for regulatory reporting, providing immutable transaction records while ensuring data integrity.

Its transparent and tamper-proof nature simplifies compliance processes and reduces the risk of financial crimes, such as fraud and money laundering. By utilising blockchain for transaction monitoring and cross-border remittances, MMPs can comply seamlessly with both local and international AML/CFT regulations, strengthening trust and fostering regulatory transparency. Ripple has implemented blockchain technology for cross-border payments, working with banks such as Banco Santander to streamline regulatory reporting and ensure transparency in international transactions. By leveraging blockchain's immutable ledger, Ripple ensures compliance with both local and international AML/CFT laws, reducing the risk of financial crimes and enhancing transparency in regulatory reporting.

---

These recommendations offer a strategic framework for MMPs to strengthen regulatory compliance and risk management. By aligning with regulators, adopting advanced technologies and fostering a risk-aware culture, providers can meet regulatory demands while advancing financial inclusion sustainably.

**GSMA Head Office**  
1 Angel Lane  
London EC4R 3AB  
United Kingdom  
+44 (0)20 7356 0600

