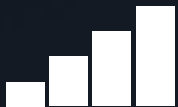
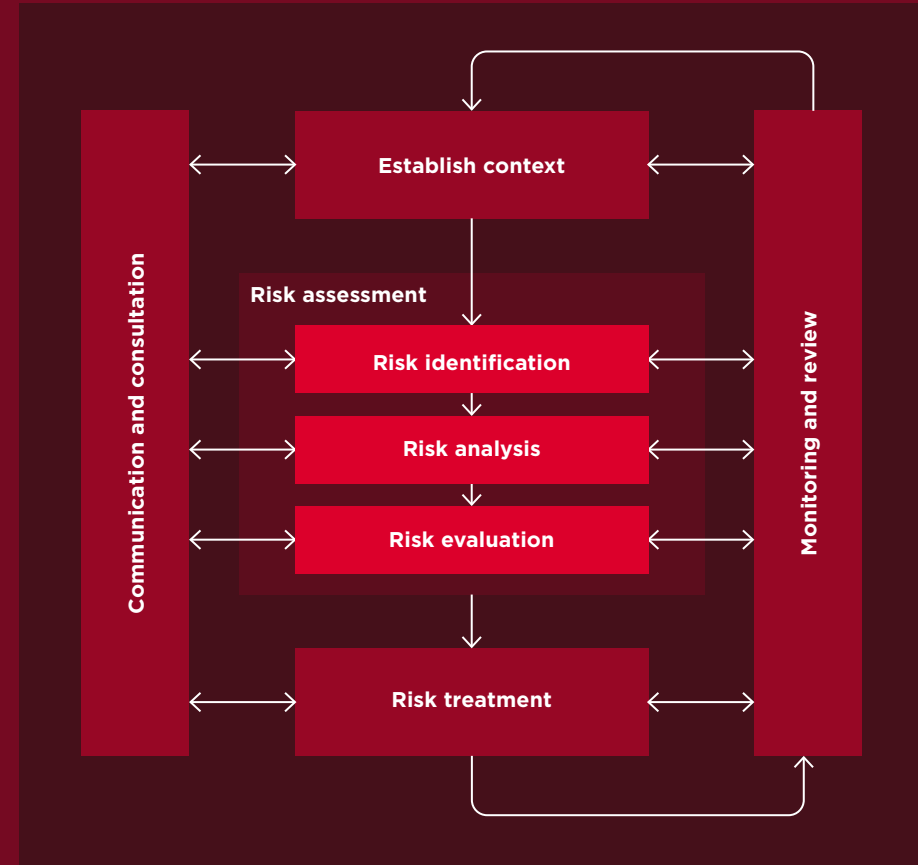
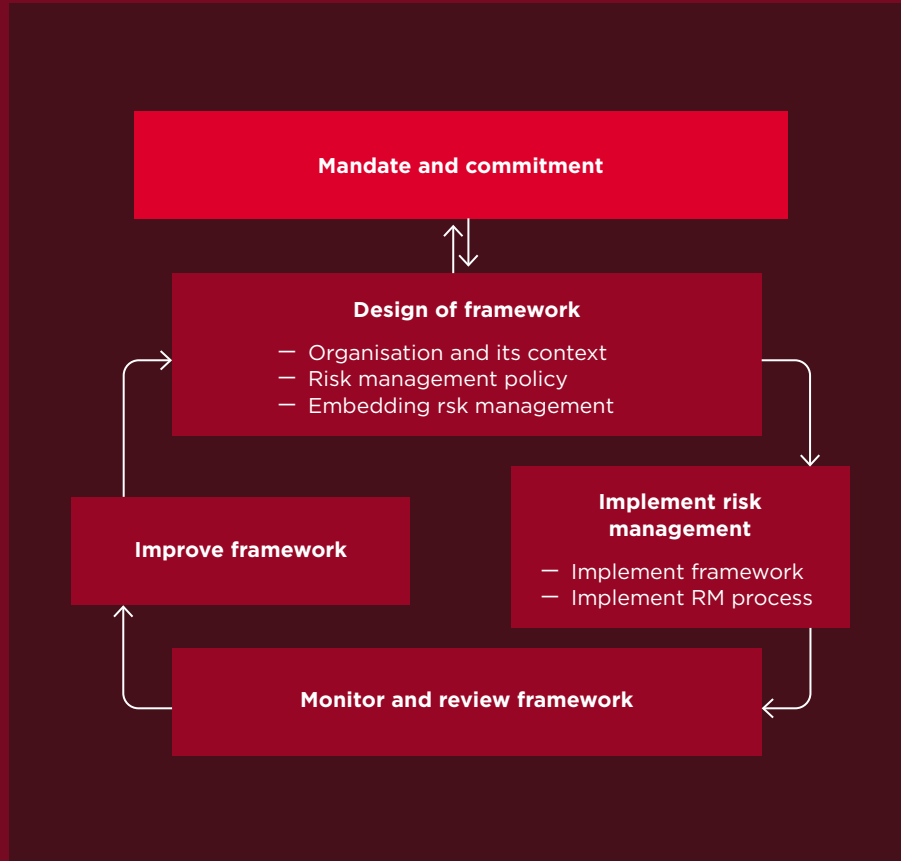


# Navigating Mobile Money Regulatory Risks

Risk Management  
Framework & Tool



# Risk Management Framework overview



# Risk taxonomy



Category	Definition
<b>▲ Reputational risk</b>	Reputational risk, shown at the centre of the diagram and therefore critical and touching all other risks, is better classified as a consequential risk. All the nine primary risks trigger events that, if unmanaged, lead to reputational harm. This perspective in DFS underscores how reputational impact is cumulative and multifaceted, directly linked to how well other risk areas are managed.
<b>01 Strategic risk</b>	This refers to the potential for losses or negative impact on an organization's goals and long-term objectives due to decisions or external changes that affect their strategic direction.
<b>02 Regulatory risk</b>	Regulatory risk is the potential for financial loss, operational disruption, or reputational damage that an organization may face due to changes in regulations, laws, policies, or non-compliance with existing regulatory requirements.
<b>03 Operational risk</b>	Operational risk is the potential for loss resulting from failures in internal processes, people, systems, or external events that disrupt normal business operations.
<b>04 Technology risk</b>	Technology risk is the potential for negative impact arising from failure in technology systems and cybersecurity threats.
<b>05 Fraud risk</b>	Fraud risk is the possibility of misrepresentation of facts or deception to the detriment of a party. Mobile money fraud is defined as fraud that takes place on assets owned or held by a mobile money service to the detriment of a mobile money service provider, its customers, agents or third parties.
<b>06 Third party risk</b>	Third-party risk is the potential for negative impacts on an organization due to reliance on external entities such as IT vendors, integrators, partners, mobile money agents or service providers for products, services, or functions. This risk arises DFS providers may not have direct control over external entities that may have different standards or priorities.
<b>07 Financial risk</b>	Financial risk refers to the potential for losses or financial instability arising from factors such as credit risk, liquidity issues, and currency fluctuations. These risks can impact a mobile money provider's profitability, cash flow, and overall financial health.
<b>08 ESG risk</b>	ESG (Environmental, Social, and Governance) risk in digital financial services (DFS) refers to the potential negative impacts associated with a DFS provider's environmental footprint, social responsibilities, and governance practice.
<b>09 Country risk</b>	Country risk refers to the potential for losses that businesses and investors may face due to events or conditions in a specific country that could adversely affect the achievement of their objectives. This type of risk encompasses a range of factors including economic, political, and social conditions unique to that country.

# Risk assessment & register

Risk ID	Risk category	Description of risks	Key Risk Indicator (KRI)	Likelihood	Financial impact	Regulatory and legal impact	Reputation impact	Weighted average impact	Risk score (impact × likelihood)	Current mitigants	Target date of implementation	Status of implementation	Mitigations implemented	Residual risk score	Other contingency plans
FRA-4	Fraud risk	Increase in fraudulent mobile money transactions	Fraudulent transaction rate	5	4	4	5	4.5	22.5	AI-based fraud detection	30/05/2025	Ongoing	Yes	Medium	Customer education campaigns
REG-18	Regulatory risk	Failure to detect money laundering activities	High Number of False Positives	4	4	5	5	4.5	18	Automated transaction monitoring & enhanced due diligence	30/04/2025	Ongoing	Partially	Medium	Regularly updating thresholds and parameters
TEC-23	Technology risk	Data breach exposing customer information	Number of security breaches	4	4	4	5	4.25	17	Multi-factor authentication & real-time monitoring	15/04/2025	In Progress	Partially	Medium	Cybersecurity insurance
OPE-21	Operational risk	Disruption due to natural disasters	Time taken to recover operations	4	3	5	5	4.25	17	Business continuity and disaster recovery plan	30/05/2025	Ongoing	Yes	Low	Remote work readiness
THI-15	Third-party risk	Dependency on a single technology provider	Vendor contract renewal risks	4	3	4	4	3.75	15	Diversified vendor relationships	30/09/2025	Planned	No	Medium	Contingency vendor contracts
REG-5	Regulatory risk	Non-compliance with data privacy regulations	Number of privacy related complaints	3	4	5	5	4.25	12.75	Data privacy governance structure	30/06/2025	In Progress	Partially	Medium	Conduct regular privacy audits
FIN-13	Financial risk	Increase in borrowing costs impacting profitability	Interest rate fluctuations	3	4	5	5	4.25	12.75	Interest rate hedging strategies	30/09/2025	Planned	No	Medium	Explore alternative and cheaper funding sources
TEC-9	Technology risk	Outdated legacy systems causing inefficiencies	Number of system errors	3	2	5	5	3.75	11.25	Invest in modern tech stack to enhance transparency	31/10/2025	In Progress	Partially	Medium	regular system audits and cloud migration strategy
OPE-8	Operational risk	System downtime impacting transactions	Downtime incidents per month	3	5	3	3	3.5	10.5	Backup servers and failover mechanisms	30/04/2025	Ongoing	Partially	Medium	Cloud-based disaster recovery
THI-24	Third-party risk	Service disruption due to vendor failure	Vendor uptime percentage	3	4	3	3	3.25	9.75	Strong SLAs with vendors	30/06/2025	Ongoing	Partially	Low	establishing strong vendor due diligence program
FIN-20	Financial risk	Revenue loss due to regulatory penalties	Total fines paid	2	5	5	5	4.25	8.5	Proactive regulatory compliance	31/08/2025	Planned	No	Low	Strengthen collaboration with regulators
REG-13	Regulatory risk	Lawsuits from customers or partners	Number of legal claims	2	4	5	5	4	8	Ensure contracts include limitation of liability and indemnification clauses.	31/07/2025	Planned	No	Low	use of standard templates
STR-29	Strategic risk	Failure to expand in high-potential markets	Market expansion rate	2	5	1	5	3.25	6.5	Strategic partnerships	31/12/2025	Planned	No	Medium	Diversification strategy
FIN-20	Financial risk	Currency fluctuations affecting cross-border transactions	Exchange rate volatility	3	4	0	0	1.75	5.25	Hedging strategies	31/07/2025	Planned	No	Medium	Automate monitoring of unhedged exposure across currencies
REP-14	Reputational risk	Negative media coverage due to system failure	Number of negative media reports	2	0	1	5	2	4	PR and crisis management plan	30/06/2025	In Progress	Partially	Low	Automate brand reputation tracking and customer support response on social media

# Likelihood rating guide

05 / 10

Rating	5 Almost certain	4 Likely	3 Possible	2 Unlikely	1 Rare
Frequency of Incidents	A significant number of incidents are likely to occur weekly	Incidents are expected to happen monthly	An incident may occur approximately once every quarter	Incidents might happen occasionally, perhaps once a year	Incidents are unlikely to occur within a year but may happen over a longer time frame
Probability of Events	<b>81-100%</b> Highly likely to materialize or with a very high frequency	<b>61-80%</b> Likely to materialize or with a high frequency	<b>41-60%</b> Could materialize or with a moderate frequency	<b>21-40%</b> Unlikely to materialize, or will with low frequency	<b>0-20%</b> Highly unlikely to materialize, or with negligible frequency

# Impact rating guide

Rating	5 Severe	4 Major	3 Moderate	2 Minor	1 Insignificant
Financial impact	\$1,000,001	\$250,001-\$1,000,000	\$100,001-\$250,000	\$5,001-\$100,000	X < \$5,000
Regulatory and legal impact	<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>
Regulatory and legal impact	<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>

# Risk scoring guide

Colour code	Risk score range	Level	Description
	<b>0-9</b>	<b>Low</b>	Minimal resources and attention, however continuously monitor to ensure they do not move to medium or high
	<b>9-12</b>	<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
	<b>12-25</b>	<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.

# Top risks on heatmap



Risk ID	Risk Category	Summarized Description	Likelihood	Impact	Risk score	Color Code
FRA-4	Fraud risk	Increase in fraudulent mobile money transactions	5.0	4.5	22.5	High
REG-18	Regulatory risk	Failure to detect money laundering activities	4.0	4.5	18.0	High
TEC-23	Technology risk	Data breach exposing customer information	4.0	4.3	17.0	High
OPE-21	Operational risk	Disruption due to natural disasters	4.0	4.3	17.0	High
THI-15	Third-party risk	Dependency on a single technology provider	4.0	3.8	15.0	High





# Read more on Navigating Mobile Money Regulatory Risks

Mobile money services have transformed financial inclusion worldwide, particularly in Africa and South Asia, by providing access to essential financial tools for underserved populations. However, alongside this revolutionary growth, new challenges have emerged. Fraud, money laundering, and cybersecurity threats are increasingly common, highlighting the need for robust and tailored risk management and regulatory frameworks.

Access the full report [here](#).



GSMA

## Navigating Mobile Money Regulatory Risks



GSMA

